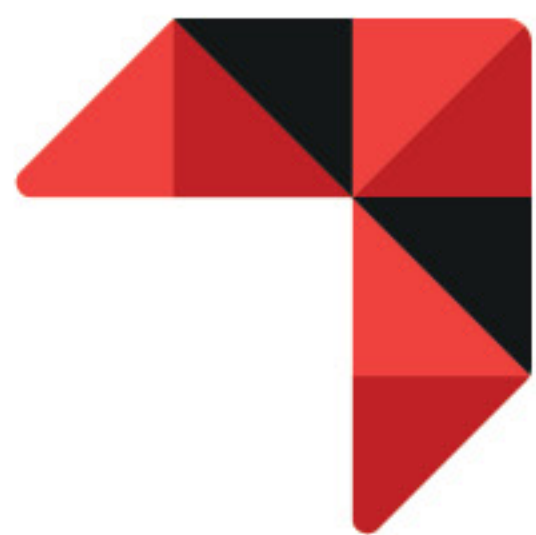




8>

Андрей КУРИЛО
мглу
Три первых шага



16>

Анатолий АКСАКОВ
Государственная Дума РФ
Итоги 2021 года

20>

Василий ПИСКАРЕВ
Государственная Дума РФ
В сторону безопасного
мира

27>

Вячеслав КАСИМОВ
Московский кредитный банк
Опыт построения
внутреннего SOC

40>

Иван ГУЗЕВ
Ассоциация ФинТех
Почему банки
не в облаках?

92>

Борис СТОЛПАКОВ
Историк криптографии
Сороковые, роковые...
И созидательные

ПРОБЛЕМА КАДРОВ. КУДА ИДЕМ?





КОНФЕРЕНЦИЯ

Информационная безопасность банков

18 апреля 2022 года

 **Москва**

Цифровое деловое
пространство



ib-bank.ru/ibb2022

+7 495 921-42-44



Игорь НЕКРАСОВ
главный редактор BIS Journal

Совсем, кажется, недавно, подводя итоги первого ковидного — 2020-го — года, мы пришли к выводу, что кое-кто от всей этой вакханалии с пандемией всё-таки выиграл. Что и зафиксировали тогда на обложке BIS Journal: «Победила цифра!» Казалось, что жизнь, неумолимо перетекающая в онлайн-формат, никогда уже не будет прежней.

А подводя итоги 2021 года, мы вдруг поняли, что не так уж всё вокруг и изменилось. Будто рассеялся какой-то цифровой морок. Мы по-прежнему издаём бумажную версию журнала, и каждый его номер рождается на бурных заседаниях нашей замечательной редколлегии. Которая, заметьте, ни разу не собиралась онлайн. Исключительно офлайн — такие уж в ней подобрались жизнелюбивые люди (сразу оговорюсь, они все проверены и привиты). Мы по-прежнему проводим офлайн-мероприятия, где люди с радостью встречаются, жмут друг другу руки, обмениваются информацией (тут тоже всё в рамках норм и правил)...

Глаза в глаза, от сердца к сердцу... Хотя и разговаривают, конечно, о цифре.

Так что же это был за морок? Наткнулся я тут на любопытное объяснение. «Если вы говорите с Богом, то это молитва, а если он с вами — это шизофрения», — написал один известный психиатр. В таком контексте процесс глобальной цифровизации можно назвать довольно интенсивным диалогом, в котором представление о конечной цели имеют явно не люди. Вот, например, искусственный интеллект. Что можно по этому поводу думать? Тот же психиатр и тут долго не рассуждает. «Ясное мышление требует мужества, а не интеллекта», — считает он.

А мужество — качество уж точно не из цифрового ряда.

Вот и мы, перестали заморачиваться, засучили рукава и занялись мужскими делами — разгребанием авгиевых конюшен в сфере ИБ. Тема этого номера — высшее образование и информационная безопасность. Её главный автор Андрей Петрович Курило — настоящий (не искусственный!) мужчина с ясным мышлением.

Работаем, товарищи!

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Войлуков А.А. — вице-президент Ассоциации банков России
Сычёв А.М. — Первый заместитель директора Департамента информационной безопасности Банка России, доктор технических наук
Шипилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А.Ю. — специалист Службы информационной безопасности КБ Максима (ООО)
Вихорев С.В. — советник генерального директора по информационной безопасности IT Expertise
Дзержинский Ф.Я. — независимый эксперт
Зубков А.Н. — генеральный директор ООО «Медиа Групп» «Авангард», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Курило А.П. — заведующий кафедрой международной информационной безопасности МГЛУ, кандидат технических наук
Левиев Д.О. — председатель Совета НП «Партнёрство специалистов по информационной безопасности»
Мельников С.Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», доктор физико-математических наук
Некрасов И.В. — главный редактор журнала
Одувалов М.В. — руководитель службы Управления по обеспечению ИБ Банка ВТБ (ПАО)
Окулесский В.А. — заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук
Пазизин С.В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО), кандидат физико-математических наук
Рачкова Е.В. — управляющий директор Управления по обеспечению ИБ Банка ВТБ (ПАО)
Филиппчук А.А. — технический директор ГК ЦРТ
Шумский Л.С. — руководитель службы информационной безопасности Яндекс Банка
Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Баранов А.П. — руководитель департамента информационной безопасности факультета информационных технологий Финансового университета при Правительстве РФ, доктор физико-математических наук, академик Академии криптографии РФ
Батранков Д.В. — консультант по информационной безопасности Palo Alto Networks
Гадарь Д.А. — вице-президент — директор департамента информационной безопасности, Tinkoff.ru
Калемберг Д.А. — генеральный директор ООО «СэйфТек»
Лукацкий А.В. — бизнес-консультант по безопасности Cisco Systems
Сабанов А.Г. — заместитель генерального директора АО «Аладдин Р.Д.»
Сумманен К.Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук
Хайретдинов Р.Н. — директор по росту компании BIZONE

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**
Директор по развитию: **Минаков А.В.**
Арт-директор: **Мельников Н.С.**
Руководитель интернет-проектов: **Воробьёва А.А.**
Ответственный редактор: **Седов О.В.**
Обозреватели: **Куликов В.А., Бродская М.А., Покатаева Е.Н.**
Иллюстрация на 1-й обложке: **Виктор Миллер-Гауса**
Фото в номере: **DepositPhotos**
Цветокорректор: **Науменко М.В.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Групп» «Авангард»
Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д.21
Тел.: +7 495 921 42 44
Интернет-версия: ib-bank.ru/bisjournal
E-mail: bis@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство ПИ № ФС77-61378 от 10 апреля 2015 г.

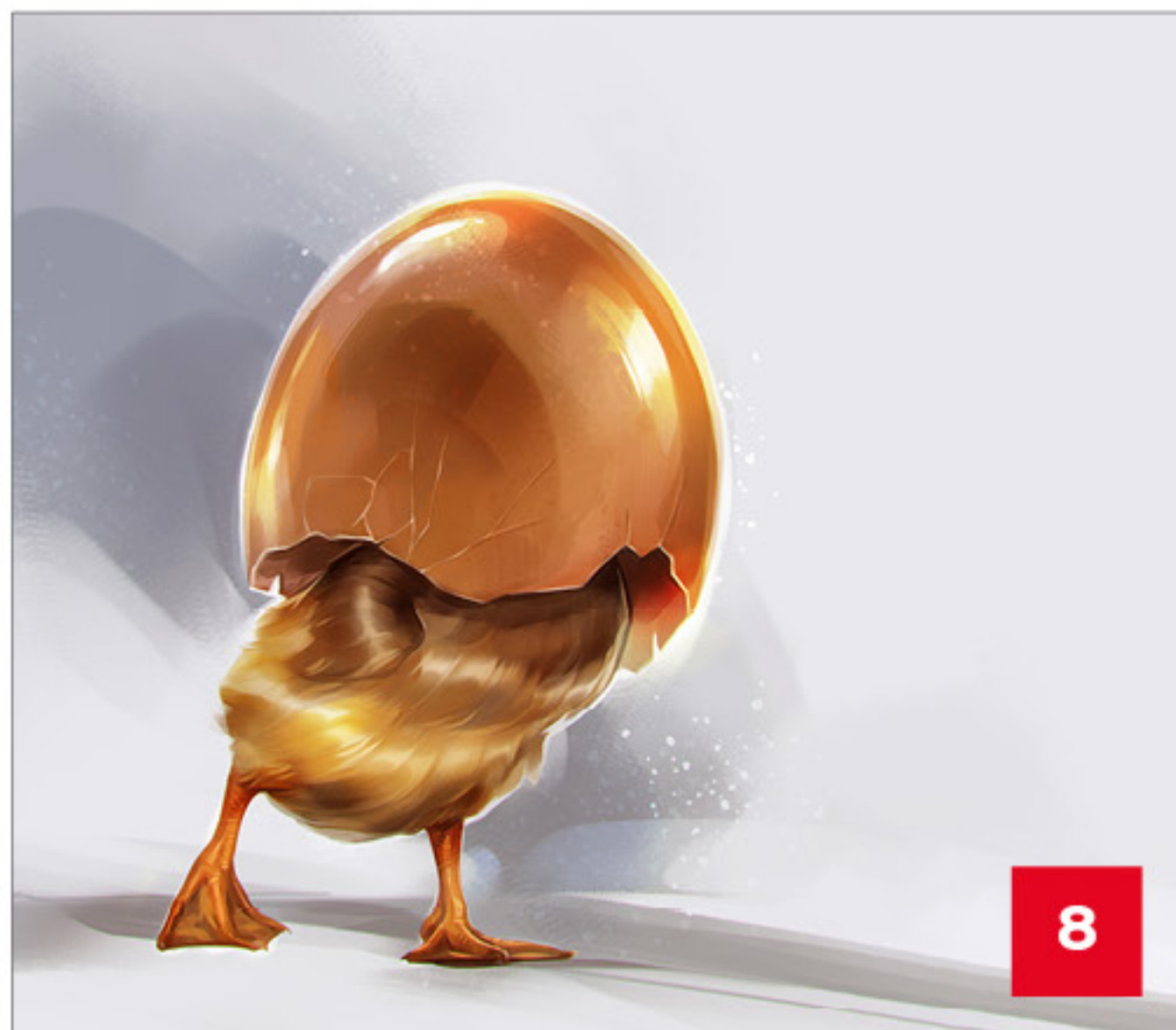
Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность банков». Перепечатка и воспроизведение иными способами без разрешения редакции запрещаются. При использовании материалов ссылка на журнал обязательна. Мнение редакции может не совпадать с мнением авторов. Присланные материалы не рецензируются и не возвращаются.

Подписан в печать 25.01.2022. Тираж 5000 экз. Заказ № 1782022. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS Journal, 2022

НОВОСТИ

5 Законодательство, криминал, технологии



ТЕМА НОМЕРА: ВЫСШАЯ ШКОЛА

8 Андрей Курило (МГЛУ) Куда идти? Три первых шага



РЕГУЛЯТОРЫ

16 Законодательство Анатолий Аксаков (Государственная Дума) Итоги 2021 года

20 Законодательство Василий Пискарев (Государственная Дума) В сторону безопасного мира

БАНКИ

24 Итоги года Никита Ломов (Ассоциация ФинТех) Финтех, который всё изменил

27 SOC Вячеслав Касимов (Московский кредитный банк) Построение внутреннего SOC

32 Опыт Сбера Иван Янсон (Сбербанк), Николай Богданов (АО «Деловая среда») РБД ОС расправляет плечи

38 Новые технологии Александр Бодрик (BIS Journal) Безопасность PROD-уровня

40 Облачные технологии Иван Гузев (Ассоциация ФинТех) Почему банки не витают в облаках?

42 Нормотворчество Константин Грачёв (КБ «Максима»), Оксана Докучаева (ГУП «Московский метрополитен»), Анастасия Николаева (КБ «АРЕСБАНК») Привести в соответствие!

44 Комментарий Сергей Вихорев (ИТ-Экспертиза) Мы с тобой два берега у одной реки...

46 Комментарий Василий Окулесский (эксперт BIS Journal) Давайте не будем делить поляну

УГРОЗЫ И РЕШЕНИЯ

- 48 Прогноз**
Александр Шмелев (AKTIV.CONSULTING)
Масштаб кибератак выводит ИБ в банках на новый уровень
- 50 Сегментация**
Вячеслав Половинко (АМТ-ГРУП)
Диоды данных
- 52 Корпоративные сети**
Александр Щетинин (Xello),
Владимир Соловьёв (ДиалогНаука)
Технология обмана
- 54 XDR-системы**
Дмитрий Нагибин (Positive Technologies)
РТ XDR снимает боль индустрии
- 56 Импортзамещение**
Дмитрий Гусев (ИнфоТеКС)
Импортзамещение в кредитно-финансовой отрасли
- 59 DevSecOps**
Андрей Муллин (СТИ)
DevSecOps. Безопасная разработка



59

ИНФРАСТРУКТУРА

- 62 Деловые мероприятия**
Алексей Лукацкий (эксперт BIS Journal)
SOC-Форум 2021
- 66 Деловые мероприятия**
Валерий Куликов (BIS Journal)
Finopolis 2021
- 68 Деловые мероприятия**
Никифор Ковалёв (BIS Journal)
Мораль как последнее прибежище ИБ
- 70 Деловые мероприятия**
Корней Реут (BIS Journal)
CyberCrimeCon 2021. Щели ада
- 72 Деловые мероприятия**
Валерий Куликов (BIS Journal)
OS DAY 2021, ROSS 2021



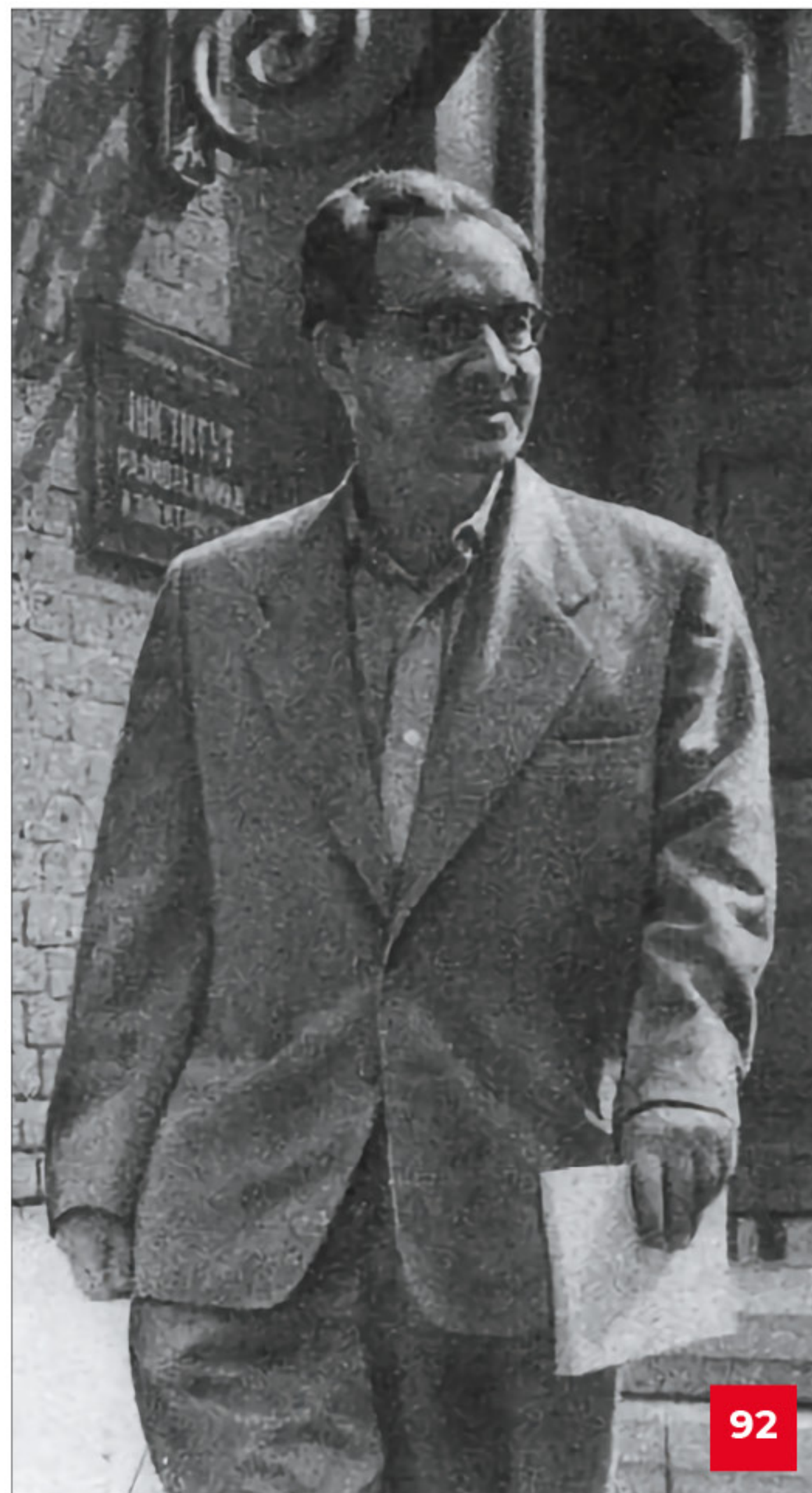
62



70

ОБРАЗОВАНИЕ И КАРЬЕРА

- 76 **За рубежом**
Марина Бродская (BIS Journal)
В ожидании штурма
- 78 **Обзор**
Анна Катанкина (BIS Journal)
Угол зрения
- 81 **Киберобзор ИноСМИ**
Марина Бродская (BIS Journal)
Виртуальная реальность становится реальной угрозой



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 84 **Опыт Сбера**
Анна Селезнева (Сбербанк)
Помоги себе сам
- 88 **Телефонное мошенничество**
Андрей Жаркевич (BIS Journal)
Ограбь меня!

СУБЪЕКТЫ

- 92 **История**
Борис Столпаков (историк криптографии)
Сороковые, роковые... и созидательные
- 98 **Отцы и дети**
Роман Мещеряков (ИПУ РАН), Валерия Мещерякова (МГУ им. М.В. Ломоносова)
От чайника до киборга
- 100 **Заметки безопасника**
Александр Бодрик (BIS Journal)
Управлять не умеем мониторить

ЦИФРОВОЙ СТАТУС ИНОСТРАНЦА В РОССИИ

Минцифры предполагает ввести статус «цифрового резидента» для ИТ-специалистов из других стран.

Такой статус позволит получить цифровое удостоверение личности — для регистрации компании, работы с финорганизациями, уплаты налогов и т.п. Однако документ не предусматривает налогового резидентства. Зарубежные айтишники, принявшие статус, смогут рассчитывать на льготы, предусмотренные недавним «налоговым маневром».

Минцифры также разрабатывает и другие меры. Предполагается: расширить налоговые льготы на интеллектуальную собственность (в России такие льготы не распространяются на такие категории продуктов, как доменные имена, товарные знаки, дизайн и т.п.); установить правила оформления дистанционной работы из-за границы; установить гибкие правила при работе ИТ-компаний с

иностранными контрагентами и минимизировать риски привлечения их к уголовной ответственности.

Сегодня по ТК в России нельзя трудоустроить человека, который не находится в стране физически. Ведомство предлагает разрешить дистанционно идентифицировать сотрудника при помощи биометрии в иностранном паспорте либо через платёжные системы, а также признать электронный документооборот между российскими и зарубежными компаниями.



ПЕРЕХОДНЫЙ ПЕРИОД ДЛЯ ЭП

Владимир Путин подписал закон, дающий юридическим лицам и индивидуальным предпринимателям право до конца 2022 года использовать ранее выданные сертификаты ЭП без машиночитаемой доверенности.

С января вступили в силу нормы, согласно которым квалифицированные сертификаты ЭП: финорганизации должны получать в удостоверяющем центре ЦБ РФ; иные юрлица и ИП — в удостоверяющем центре ФНС; госслужащие — в удостоверяющем центре Федерального казначейства; а граждане (не должностные лица) — в коммерческих удостоверяющих

центрах, аккредитованных после 1 июля 2020 года.

Подписанный закон переносит начало применения норм об использовании машиночитаемой доверенности на 1 марта и допускает использование ранее выданных без такой доверенности сертификатов ЭП до конца 2022 года.

Так устанавливается переходный период: можно будет применять либо новый режим, когда используется простой квалифицированный сертификат ЭП вместе с машиночитаемой доверенностью, либо использовать сертификат с указанием в нём полномочий представителя, как прежде.



«ГУЛЯЮТ ВСЕ!»

Банк России разработал проект закона, разрешающего нефинансовым компаниям оказывать платёжные услуги. В БР считают, что реализация этой инициативы улучшит качество и доступность услуг для потребителей. Также регулятор готовится обсудить поправки в законодательство с самими компаниями.

По плану, организации разделят на два типа НППУ (небанковских поставщиков платёжных услуг): первые смогут проводить транзакции с согласия клиента (сумма их активов должна быть не менее 5 млн руб.); вторые — смогут самостоятельно организовывать переводы и открывать электронные кошельки для предприятий малого и среднего бизнеса (сумма их активов — не менее 50 млн руб.).

Кроме того, БР введёт понятие платёжного агрегатора — для него установлен минимальный порог в 10 млн руб.



КОДЕКС ЭТИКИ ДЛЯ ИИ

Совет Федерации планирует закрепить в законодательстве Кодекс этики в сфере искусственного интеллекта.

Совет Федерации — предположительно — хочет предложить ввести отдельный запрет на использование в ИИ-сфере алгоритмов и параметров, которые дискриминируют граждан по различным признакам, а также рекомендовать Министерству экономики разработать механизм, оценивающий последствия внедрения ИИ с точки зрения негативного воздействия на права человека.

Базовые положения морали для ИИ могут вписать в отдельный федеральный закон либо в закон «Об информации, информационных технологиях и о защите информации».

ПО ДВУМ СТАТЬЯМ

Андрею Новаку, главе международной хак-группы Infracore Organization, ранее объявленному ФБР в розыск и задержанному российскими правоохранителями, предъявили обвинение. Как и другим фигурантам уголовного дела.

«Всем фигурантам предъявлено обвинение в совершении преступлений, предусмотренных частью 2 статьи 187 УК РФ (неправомерный оборот средств платежей) и частью 2 статьи 272 УК РФ (неправомерный доступ к компьютерной информации)», — рассказали в пресс-службе Тверского суда Москвы.

Новак арестован до 18 марта. Трое предполагаемых подельников — Константин Бергман, Марк Бергман и гражданин Эстонии Кирилл Самокутяев — отправлены под домашний арест до той же даты. Мера пресечения пока не обжалована. Следствие продолжает устанавливать других членов группировки.

С КОРСЧЁТА В ЦЕНТРОБАНКЕ...

В Group-IB рассказали, что хак-группа MoneyTaker похитила средства российской кредитной организации с её корсчёта в Банке России.

Название банка и точная сумма не сообщаются, но безопасники отмечают, что для операций такого рода за последние годы этот инцидент оказался самым чувствительным. По некоторым данным, ущерб составил более полумиллиарда рублей.

Кибератаку провели через автоматизированное рабочее место банка в Центральном банке Российской Федерации ещё в июне прошлого года; предположительно, через физическое устройство, установленное в аффилированной сети. Далее злоумышленники получили доступ к банковской сети и на протяжении полугода исследовали её. В январе уже этого года они получили доступ к системе межбанковских переводов и украли цифровые ключи.

ЗА ЧТО ОШТРАФОВАЛИ GOOGLE

Председатель Комитета ГД по безопасности и противодействию коррупции Василий Пискарев прокомментировал сообщение о наложении российским судом на компанию Google оборотного штрафа в сумме 7,2 млрд руб. Его слова цитирует telegram-канал Комитета <https://t.me/bzpasn>:

«Любая работа в Интернете должна находиться в правовом поле. Тем более если иностранная компания предоставляет услуги в России, получает хорошую прибыль, то она обязана по закону обеспечивать безопасность пользователей, в первую очередь — детей — от запрещённой информации.

Последовательная деятельность всех ветвей власти по принуждению IT-гигантов к соблюдению закона говорит о том, что Россия не позволит кому бы то ни было диктовать свои условия, работая в российском информационном пространстве, и подтверждает решимость государства

добиваться соблюдения законодательства от всех участников рынка.

О необходимости привести распространяемый на российскую аудиторию контент в соответствие с нашим законодательством, удалить материалы, содержащие детскую порнографию, пропаганду суицида и наркотребления, руководству Google неоднократно говорили депутаты Государственной думы, в том числе в ходе общения с руководством компании в апреле и октябре текущего года. Рынок России открыт для каждого, в том числе и для Google, мы добиваемся лишь одного — исполнения и уважения наших законов».



С ГОРЫ ДЕНЕГ НА НАРЫ

Центр общественных связей ФСБ России сообщил, что сотрудники службы задержали вымогательскую хак-группу REvil в полном составе (14 человек).

«Федеральной службой безопасности во взаимодействии со Следственным департаментом МВД России в Москве, Санкт-Петербурге, Московской, Ленинградской и

Липецкой областях пресечена противоправная деятельность членов организованного преступного сообщества», — отметили в ЦОС. И добавили, что основанием послужило обращение компетентных органов США.

Американская сторона ранее сообщала о причастности лидера REvil к атакам на информресурсы зарубежных техгигантов (внедрение зловредов, шифрование информации и вымогательство денег за дешифровку).

По данным ФСБ, задержанные разрабатывали вредоносный софт, организовывали хищение денежных средств со счетов иностранных граждан и обналичивали их, нередко путём приобретения дорогостоящих товаров онлайн.

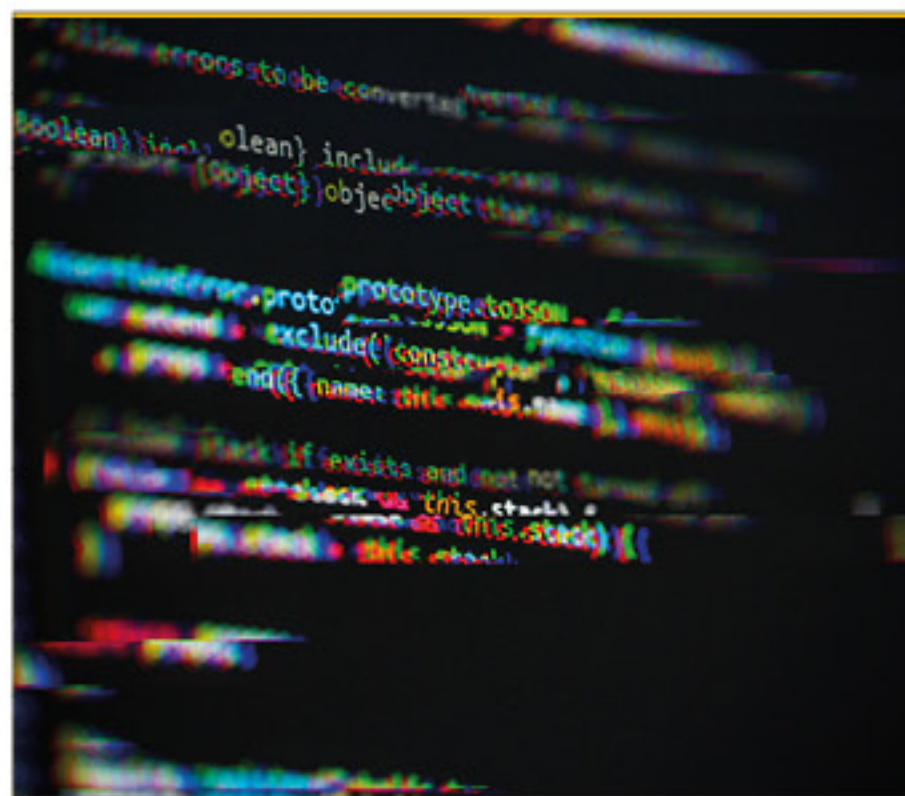
По 25 адресам мест пребывания членов хак-группы было изъято более 426 млн рублей (в том числе в криптовалюте), 600 тыс. долларов, 500 тыс. евро, компьютерная техника, криптокошельки и 20 премиальных автомобилей.



«ФАНТОМ» ГОТОВИТСЯ К ПОЛЁТУ

Рабочий прототип российской ОС «Фантом» может появиться уже в этом году, сообщил гендиректор компании-разработчика операционной системы, холдинга DZ Systems, Дмитрий Завалишин. Работа над проектом ведётся с 2010 года.

Завалишин уточнил, что основная версия ОС уже готова к пилоту, а работа над версией для Genode ещё продолжается.



«На сегодня существует базовая версия ОС «Фантом», которая включает в себя два слоя — традиционный слой кода, который управляет «железом» компьютера, и собственно слой реализации сущности ОС. Первый слой — это работа с процессором, контроллером памяти, драйверы устройств и т.п. Всё это есть в любой ОС. Работа по портированию заключается в замене первого слоя на аналог из Genode. В процедуру входит написание прослойки, которая реализует низкоуровневые примитивы ядра ОС «Фантом», которые, в свою очередь, реализованы через аналогичные примитивы ядра Genode», — рассказал глава DZ Systems.

Заявлено, что «Фантом» разрабатывается с нуля, базируется на концепции персистентной виртуальной памяти, ориентирована на управляемый код, нацелена на применение в носимых и встроенных компьютерах, а также работает по принципу «всё есть объект».

IPHONE СТАНЕТ ТЕРМИНАЛОМ

Apple готовится наделять iPhone правами платёжного терминала. Известно, что разрабатываемая функция будет завязана на NFC (Near field communication), который используется для оплаты с помощью Apple Pay, — компания добавит её в iOS «в ближайшие месяцы». Пока что «яблочный» смартфон можно использовать для приёма оплаты, только подключив его к внешнему терминалу.

Новое решение позволит техгиганту конкурировать с крупнейшим производителем платёжных терминалов — Square. Ещё неясно, будет ли функция частью Apple Pay, однако есть данные, что разработчики Mobeewave работали именно в этом подразделении (летом 2020 года Apple купила разработчика платёжного приложения Mobeewave, чей продукт превращает любой смартфон в самостоятельный платёжный терминал).



iFin-2022

XXII МЕЖДУНАРОДНЫЙ ФОРУМ

8-9 февраля 2022, г. Москва
«Рэдиссон Славянская»

Электронные финансовые
услуги и технологии

18+

Спонсоры



Партнеры



Форум iFin-2022 – это центральное мероприятие в России, посвященное электронным финансовым услугам и технологиям, которое проводится ежегодно с 2001 года. Организатор Форума – Компания «АйФин медиа» при поддержке Ассоциации российских банков.

Тематические акценты Форума iFin-2022

- Новейшие решения в сфере ДБО, интернет/мобильного банкинга и трейдинга
- Автоматизация обслуживания физических лиц, самозанятых, МСБ и корпораций
- Совершенствование ИТ-инфраструктуры и цифровизация бизнеса
- Информационная и кибербезопасность
- Современные инструменты коммуникации с клиентами
- Развитие СБП, платёжных решений и сервисов
- Цифровой профиль и биометрия, цифровизация финансовых сервисов
- Развитие маркетплейсов, экосистем и открытого банкинга
- Технологии привлечения и удержания клиентов, укрепления лояльности
- Практическое применение Big Data, AI, Open API, блокчейна в финансах



КУДА ИДТИ? ТРИ ПЕРВЫХ ШАГА

И СНОВА О ПОДГОТОВКЕ В ВЫСШЕЙ ШКОЛЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ¹

К вопросу растущего дефицита кадров в области информационной безопасности мы уже обращались. Пока, к сожалению, и реакции практически нет, да и результатов особо не видно, хотя нельзя не отметить, что наши образовательные власти кое-что делают в этом направлении. Да и госструктуры и ведомства, от которых как-то зависит решение вопроса, тоже прилагают определённые усилия. Насколько эффективные — об этом речь пойдёт ниже.

ПОЛОЖЕНИЕ ВЕЩЕЙ

Мы поставили перед собой задачу взглянуть на эту сферу деятельности ещё раз и надеемся, что это может в какой-то степени помочь решению столь непростой проблемы.

Формально всё выглядит неплохо. В стране, по данным Федерального учебно-методического объединения в системе высшего образования по УГСН 10.00.00 «Информационная безопасность» (УМО), в настоящее время около 150 вузов готовят специалистов по Федеральным образовательным стандартам по информационной безопасности (ФГОС) 10.03.01, 10.04.01 и 10.06.01. Точными цифрами мы не располагаем, но если каждый вуз выпускает хотя бы 50 специалистов в год, то на рынке ежегодно появляется более 7500 новых работников. Если в этой сфере деятельности в специальности остаётся, по очень неточным данным (точной статистики нет, она не ведётся), 10–20% выпускников, то мы имеем от семисот до полутора тысяч реальных работников каждый год. Этого, конечно, мало. При этом мы видим, что регуляторы в сфере образования и УМО озабочены уровнем подготовки студентов и критически оценивают качество образования по ИБ в ряде вузов. Отсюда

и планы по сокращению их числа, централизации подготовки в крупных технических образовательных учреждениях, созданию, усилению и укреплению учебной материально-технической базы, введению новых ФГОС, изменению правил аккредитации по образовательным программам и т.д.

С целью приближения к потребностям рынка образования и знаний выпускников в 2016 году Минтруда выпустило профессиональные стандарты, определяющие группы занятий и обобщённые и конкретные трудовые функции для специалистов, работающих в следующих областях:

- ◆ 06.030 «Защита информации в телекоммуникационных системах и сетях, включая сети связи специального назначения»;
- ◆ 06.031 «Автоматизация информационно-аналитической деятельности»;
- ◆ 06.032 «Обеспечение безопасности компьютерных систем и сетей»;
- ◆ 06.033 «Защита информации в автоматизированных системах»;
- ◆ 06.034 «Техническая защита информации».

Центральным банком подготовлен проект профессионального стандарта «Специалист по защите информации в кредитно-финансовой сфере».

Новая редакция ФГОС 10.03.01, 10.04.01, версия 3++ предусматривает существенное усиление требований к вузам по части дисциплин, подлежащих обязательному изучению, (что ведёт к унификации обучения студентов на первых курсах в различных вузах), ужесточение требований к квалификации профессорско-преподавательского состава и, наконец, повышение требований к практической подготовке студентов в профильных предприятиях и организациях.

Решил отметить и Минобрнауки, введя критериальные механизмы оценки качества и уровня знаний и умений, получаемых студентами высшей школы через введение системы оценки качества образования на основе новых



Андрей КУРИЛО
заведующий
Кафедрой
международной
информационной
безопасности
МГЛУ, кандидат
технических наук,
доцент

¹ Автор выражает признательность Сергею Владимировичу Пазизину, заместителю начальника Управления по обеспечению ИБ Банка ВТБ (ПАО), к.ф.-м.н., доценту, за анализ и весьма ценные замечания, высказанные в ходе работы над данной статьей

понятий: компетенций, дескрипторов и индикаторов. Также с завидной регулярностью меняются требования и форматы базовых документов: образовательных программ, рабочих программ дисциплин, всякого рода учётных и отчётных документов. Нет сомнений, что всё это направлено на благое дело — повышение качества образования, качества работы профессорско-преподавательского состава и усиление контроля за образовательным процессом.

Делается эта работа как всегда быстро, в результате чего образовательные учреждения попадают в трудное положение, будучи вынуждены срочно переосмысливать и переделывать сотни весьма сложных документов, регулирующих и регламентирующих образовательный процесс. Пока единственный видимый результат — дальнейшее усиление бюрократизации и существенное увеличение нагрузки на людей.

Появились гранты Минобрнауки и негосударственных фондов, призванные повысить качество образовательных программ и как-то улучшить финансовое положение молодых преподавателей и учёных.

На этом фоне весьма хорошо чувствуют себя коммерческие образовательные учреждения, гораздо менее связанные с формальностями и быстро реагирующие на «злобу дня» своими узко заточенными программами дополнительного образования. Но они не смогут заменить классическое высшее. Да так и не ставится задача.

И В ТО ЖЕ ВРЕМЯ...

Повторимся, всё внешне выглядит неплохо. Но при этом дефицит специалистов на рынке меньше не становится, а растёт, и уровень подготовки новоиспечённых бакалавров, а иногда и магистров, порой сильно огорчает практиков. К тому же, как ранее отмечалось, в специальности остаётся 10–20 % выпускников. При этом, по последним данным компании HeadHunter, число вакансий в сфере информационной безопасности (ИБ) в России выросло в 2021 году на 47 %, а их общее количество

составило 35,3 тысячи. Почти треть из них относятся к сегменту IT-компаний и системных интеграторов (рост в 31 % внутри отрасли). Помимо них, в лидерах оказались финансовый сектор (55 %) и отрасль телекоммуникационных услуг и связи (43 %). Также отмечается снижение интереса к вакансиям со стороны кандидатов, что говорит о снижении конкуренции. Это, мягко говоря, плохо и отражает наличие глубоких нерешённых проблем в сфере подготовки кадров для деятельности, без которой вся та самая цифровизация, о которой мы так усердно говорим, превратится в своего антипода и способна создать нашему обществу вместо благ и движения вперед очень большие трудности. Об этом в голос трубят факты: и последние громкие инциденты, и растущий у идеологов цифровизации правовой нигилизм и резкий рост киберпреступлений. Об этом говорят и уважаемые эксперты в области информационной безопасности и информатизации — Н. Касперская и И. Ашманов.

Но попытаемся пристальней взглянуть на проблемы подготовки кадров.

КОГО ГОТОВИМ? И ДЛЯ ЧЕГО?

Начнём с простого вопроса: а кто нужен рынку; кого нужно готовить; какими компетенциями, как сейчас модно говорить, должен обладать специалист в области информационной безопасности?

Для этого сначала нужно присмотреться к самой сфере информационной безопасности в России. Несмотря на идущие в ней процессы централизации и вытеснения малых предприятий, состоит она из нескольких секторов:

- ◆ производства средств и систем защиты, включая взаимодействие с регуляторами в части сертификации продукции (вендоры);
- ◆ предоставления услуг по созданию, комплексированию и модернизации систем защиты (системная интеграция);
- ◆ аудита и консалтинга в сфере ИБ;
- ◆ целевых услуг по аналитике социальных сетей и интернет-разведке, мониторингу угроз и уязвимостей, управлению системами безопасности, расследованию киберпреступлений, обработке и хранению данных, вычислительным услугам и т.д.);
- ◆ собственно потребителей услуг и сервисов безопасности — предприятий промышленности, бизнес-структур, крупных корпораций, финансовых организаций, операторов связи, государственных органов и структур и т.д.

Какие специалисты и с какими знаниями там нужны?

Начнём с простого вопроса: а кто нужен рынку; кого нужно готовить; какими компетенциями, как сейчас модно говорить, должен обладать специалист в области информационной безопасности?

ЧИТАЕМ ПРОФСТАНДАРТЫ

Профстандарты, выпущенные Минтрудом 6 лет назад, а принятые к разработке ещё на несколько лет раньше и потому объективно устаревшие, весьма путано отвечают на этот вопрос, так как почти во всех этих документах присутствует целая группа практически одинаковых профилей специалистов, возможно актуальных на 2016 год. Но времена уже изменились. К тому же внимательное прочтение этих документов приводит к следующим выводам.

Налицо глубокое пересечение сфер регулирования, так как крайне сложно, например, провести четкую границу между компьютерными системами, сетями и автоматизированными системами, так как это суть одно и то же, правда, в одном случае необходимо обеспечивать защиту информации, а в другом — обеспечивать безопасность. Если не иметь в виду физическую охрану, то эти понятия — синонимы. Почти полностью накладывается, с некоторым исключением, на эти области сфера регулирования стандарта 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», а проблематика автоматизации информационно-аналитической деятельности за прошедшие годы приобрела совершенно иное значение, о котором в действующем стандарте 06.031 «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности» вообще нет упоминания. Возникает естественный вопрос: а как включить эти стандарты в соответствующие образовательные программы с точки зрения сопряжения терминологии, используемой во ФГОС (компетенции-дескрипторы-индикаторы) с терминологией профессиональных стандартов (группа занятий — вид экономической деятельности — общая трудовая функция — трудовая функция).

Содержание общих и просто трудовых функций по всем стандартам существенным образом пересекается, что говорит о явной отраслевой фрагментации общей задачи. Это застарелая проблема регулирования сферы информационной безопасности.

ВЫЯВЛЯЕМ ПОТРЕБНОСТИ РЫНКА

Тем не менее, анализируя потребности рынка совместно с имеющимися профессиональными стандартами, можно выделить основные профили или виды деятельности, по которым очевидно и нужно готовить специалистов с высшим образованием в области информационной безопасности.

Эти профили, по нашему мнению, следующие.

Анализируя потребности рынка совместно с имеющимися профессиональными стандартами, можно выделить основные профили или виды деятельности, по которым и нужно готовить специалистов

♦ Специалист по управлению (подпрофили: методолог, руководитель по направлению деятельности, специалист по документированию, специалист по защите персональных данных, специалист по защите КИИ). При этом понятно, что готового руководителя в стенах вуза подготовить невозможно, это опасное заблуждение, руководитель вырастает в ходе практической работы. Но основные знания и компетенции в области управленческой деятельности в сфере управления в области информационной безопасности молодому человеку заложить вполне возможно;

♦ Аналитик по безопасности автоматизированных систем (подпрофили: специалист по архитектуре защищенных информационных систем, аналитик кода, аналитик защищенности автоматизированных информационных систем);

♦ Аудитор информационной безопасности;

♦ Специалист по обеспечению информационной безопасности (подпрофили: специалист по криптографическим методам защиты и применению сервисов PKI, специалист по защите сетевой инфраструктуры, специалист по технической защите информации);

♦ Специалист по инцидентам информационной безопасности;

♦ Специалист по расследованию киберпреступлений;

♦ Аналитик данных средств социальной коммуникации;

♦ Системный архитектор, разработчик.

В этом перечне нет отраслевой привязки, так как профили являются универсальными. Отраслевую привязку целесообразно делать на уровне профильных учебных заведений.

ТРИ ВОПРОСА И РЕАЛЬНАЯ СИТУАЦИЯ

В этой связи, учитывая востребованные профили специалистов, уместно задать три вопроса:

1) Как и чему учить студентов? Этот вопрос весьма сложен и требует отдельного, более детального рассмотрения, анализа и обсуждения на уровне отдельной статьи.

2) Как и какими силами организовать и обеспечить качественный учебный процесс?

3) Что улучшить в обеспечении учебного процесса?

Отметим, что проблема эта многогранная. Сама проблематика информационной безопасности демонстрирует быструю изменчивость и вариативность, к тому же имеет тенденцию к расширению предметной области. Изменения в сфере ИБ и новые направления возникают быстро, буквально в течение 2–3 лет. Образовательные учреждения просто не успевают за ними, в результате чего не происходит научного и методологического осмысления возникающих вопросов. Особо следует отметить, что эти знания часто не формализованы и не описаны, следовательно, плохо доступны для сообщества. Основным методом обмена этими знаниями — участие в профильных конференциях, особенно в их неформальной части. В результате адаптация ФГОС и образовательных программ образовательными учреждениями по понятным и объективным причинам отстаёт от практики.

И ещё раз подчеркну, что практический опыт и знания в этой сфере, а значит, и результаты осмысления, накапливаются у практикующих специалистов, как говорят, «на кончиках пальцев». Как донести эти знания до студентов и превратить в их компетенции?

И тут во весь рост встает две проблемы: качество профессорско-преподавательского состава и получение студентами твёрдых практических знаний. Напомним, что рынок нуждается в специалистах, владеющих тонкостями проблемы, а не в людях, имеющих общее представление о проблеме.

ПРЕПОДАВАТЕЛЬСКИЙ СОСТАВ

Преподаватели высшей школы, как мы знаем, делятся на две категории:

1) Штатные работники, связавшие свою жизнь с преподаванием в высшей школе. Их профессиональный рост, статус, рейтинг и финансовое положение реализуются во вполне определённых рамках, предполагающих наличие учебной нагрузки, ученой степени, научного звания и количества публикаций. Эта парадигма прекрасно работает в устоявшихся «академических» отраслях знаний. Обеспечение материального благополучия вполне возможно, однако требует, как уже отмечалось, большой учебной нагрузки, ведения деятельности по получению учёных степеней и званий, написанию большого числа статей в индексируемые журналы и т.д. То есть, времени и средств, чтобы разобраться в



хитросплетениях проблематики, нет. К тому же преподаватели перегружены отчетностью. Всё это практически исключает для них возможность повышения профессиональной компетенции путем участия в практических работах совместно с практикующими специалистами по решению наиболее острых вопросов в области ИБ. Может быть по этим причинам, может быть и нет, но личный опыт автора по привлечению к практической деятельности преподавателей высшей школы всегда был неудачным.

2) Вторая категория преподавателей — совместители, среди которых выделяется группа специалистов рынка, владеющих именно теми знаниями, которые возникают в профессиональной сфере деятельности. Эти специалисты не заинтересованы в переходе в высшую школу. Во-первых, по причине отрыва от практики, что их неминуемо профессионально ослабит, и, во-вторых, по причине крайне скудного финансирования этой категории специалистов



в системе высшей школы. К тому же работать с серьезной учебной нагрузкой они не могут по причине занятости на основной работе и часто не имеют достаточной практики преподавания. Составление учебных программ и разработка учебных пособий превращается в муку для них и методистов кафедр. А те небольшие часы, которые они тратят на передачу своих знаний «на кончиках пальцев», оплачиваются по общим тарифам. Только единицы этих людей имеют учёные степени, звания и публикации. Это заведомо выводит данную категорию преподавателей на проигрышные позиции в принятом в высшей школе профессиональном рейтинге. Естественно, что такой переход неминуемо ухудшает их материальное положение и статус. Вот и получается, что ведущие специалисты-практики получают за передачу своих очень важных знаний студентам сущие копейки, вызывающие разве что смех. Далеко не каждый готов работать в таких условиях. При этом,

новые ФГОСы 3++ приветствуют привлечение совместителей, и даже предполагают доведение их числа до 50%, от общего состава кафедр, реализующих соответствующие программы обучения, однако по причине отсутствия у них степеней и званий учебное заведение одновременно нарушает требования того же ФГОС по проценту остепенённых преподавателей. Возникает замкнутый круг.

Разорвать его можно только путём принятия серьёзных системных решений, например, приравнивания квалификации специалиста с рынка уровня, соответствующему степени и научному званию преподавателя высшей школы, а выполненные успешно работы и бизнес-проекты — соответствующим статьям в научных изданиях. Ну, и конечно, стоимость часа занятий для таких специалистов должна быть установлена хотя бы в 2 раза выше, чем сейчас. Это будет ниже, чем в коммерческих организациях, но свою задачу решит, преподаватели найдутся.

О ПРАКТИЧЕСКИХ НАВЫКАХ СТУДЕНТОВ

Далее — твёрдые практические знания могут быть получены студентами только двумя способами:

- 1) в ходе прохождения практики в профильных организациях;
- 2) в ходе выполнения лабораторных работ на современной учебной базе.

О ПРАКТИКЕ

Дела с организацией и прохождением практики обстоят весьма не просто. Платное специализированное повышение квалификации с выдачей соответствующего, признаваемого рынком, сертификата есть и широко развито, а вот с практикой студентов в профильных организациях — проблемы.

Министерство образования ужесточает требования к её прохождению, повышая ответственность образовательных учреждений. Это, вне всяких сомнений правильно. Однако на рынке далеко не все профильные организации горят желанием принимать практикантов. У некоторых есть специальные программы и специальные люди для организации такой работы, но это собственные, как правило платные программы, не согласующиеся с ФГОС. Понятно, что эти программы нацелены на подбор кандидатов на работу, а не на обучение студентов.

Поэтому представитель образовательного учреждения, пытаясь пристроить на практику своих студентов — а их может быть много — натывается на предложение сначала провести собеседование, тестирование, то есть отобрать небольшую группу, а потом уже приступить к собственно проведению практики.

Вызывает вопросы сам процесс прохождения практики, он требует организации и сопровождения, работы с практикантами. Свободных ресурсов на обеспечение этой деятельности как правило у фирм нет. В последнее время крайне сложно выстраивается формальная сторона вопроса организации практики, начиная с подписания договоров, которое превращается в «дуэль юристов», отнимающую время, а его и так

не много. И, пожалуй, главное — это сложность привлечения к сотрудничеству коммерческих фирм, они не видят и не ощущают своей заинтересованности в этом процессе. А государство, ужесточая требования к вузам в этой части, не включило рынок в состав заинтересованного субъекта, установив таким образом одностороннюю ответственность.

В целом организация практики — тяжелый процесс, занимающий львиную долю времени преподавателей и организаторов.

Вместе с тем, по мнению и преподавателей и принимающих сторон, практика — это ключевой элемент подготовки будущих специалистов. Объём её нужно не уменьшать, а наоборот — увеличивать.

Уместно задать вопрос: а каков практический результат этой деятельности в складывающихся условиях и как её радикально улучшить. Ответ не радует — практически никак. Опять замкнутый круг.

Однако и решение очевидно: коль скоро государство заинтересовано и взяло на себя ответственность по организации подготовки специалистов, деятельность по проведению практики в профильных организациях должна быть материально и финансово поддержана. В идеальном варианте, образовательное учреждение должно иметь возможность заключать с профильными организациями финансовые договоры, делающие эту работу привлекательной для рынка. Тогда и организаторы сразу найдутся, и помещения, и руководители практик и результаты сразу будут видны. Самое интересное, что цена таких договоров совсем небольшая, а вся работа легко поддается планированию в нашей бюрократической системе. Нужно только смелее принимать решения. От этого много зависит.

О МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЕ

Следующий вопрос: на какой учебно-материальной базе готовить студентов?

ФГОС устанавливает только самые общие требования к ней. В этой связи вспоминается забытый старый опыт высшего военного образования в СССР, когда военные училища первыми получали новейшие образцы техники и вооружения, которых ещё не было в войсках. Зато потом специалисты получались, которых не нужно было переучивать как минимум 8–10 лет. Вот это был взгляд в будущее.

А чем мы хуже? Или уже не можем?

Ответ тут очевиден: для того, чтобы подготовить специалистов, владеющих упомянутыми выше компетенциями, нужна самая

Вспоминается забытый старый опыт высшего военного образования в СССР, когда военные училища первыми получали новейшие образцы техники и вооружения, которых ещё не было в войсках

современная, специализированная и довольно дорогостоящая материальная база. Где, что и у кого её взять, мы знаем. Как и чему учить, тоже. Конечно, научить студентов работе на всех средствах и системах безопасности невозможно и нецелесообразно, но они должны быть знакомы с основными классами средств и систем защиты, методами, принципами и приемами администрирования безопасности сетей, систем и баз данных и виртуальных сред, с методами и способами выявления и управления инцидентами в основных типах информационных систем, обработки и анализа данных систем управления безопасностью или систем социальной коммуникации, методами и приемами тестирования систем безопасности и выявления уязвимостей. Это вполне по силам, с учётом выбранного профиля подготовки.

А вот вопрос о том, как получить такую материальную базу остаётся открытым. Вузам сложно её приобрести из собственных средств, особенно, если они исторически не специализировались в области IT-технологий. Снова тупик. Даст ли результат сверхконцентрация обучения в нескольких крупных образовательных центрах? Вопрос. Перенос центра тяжести в регионы — дело хорошее, но где там преподавателей взять? Ведь практически вся интеллектуальная элита в сфере ИБ сосредоточена в столице и ещё двух-трёх городах.

ПОКА ЛАТЕНТНАЯ СТАДИЯ

Отметим также, что информационная безопасность — это не строгая математическая дисциплина, а целая практическая «политехническая» отрасль, опыт и знания в которой возникают у практикующих специалистов «на кончиках пальцев». Отрасль с колоссальным числом разного рода ответвлений и направлений — от очень серьёзной криптографии, исследований кода и программирования, до вопросов управления, аудита, оценки рисков, анализа уязвимостей, трассировки атак и социальной инженерии. В целом, по широте охвата и числу прикладных направлений, она поразительно напоминает медицину. А там иная система подготовки студентов, и есть даже своя Академия наук.

В целом всё перечисленное крайне негативно влияют на общую ситуацию. Поневоле на ум приходит сравнение с тяжелой опасной болезнью, признаки которой сначала не видны, латентны, но именно в это время её можно вылечить. Потом поздно. Ничего не помогает.

Выходов из этой проблемы два: либо дальнейшая формализация и усиление требований

По широте охвата и числу прикладных направлений информационная безопасность поразительно напоминает медицину. А там иная система подготовки студентов, и есть даже своя Академия наук

к образовательным учреждениям, что ещё больше усложнит проблему, либо творческая переработка поставленной задачи.

ПОДВОДНЫЙ КАМЕНЬ СТАНДАРТИЗАЦИИ

Вообще, представляется, что интенсивная детализация процесса обучения и его последующая стандартизация может стать опасным явлением. Ведь стандартизация, если вернуться к сути этого процесса, предназначена для закрепления типовых и отработанных действий, условий или требований, приводящих в итоге к обеспечению единого, стандартного уровня качества выпускаемой продукции или предоставляемых услуг. А нам нужны ещё и творческие личности, способные к неформальным и быстрым действиям, это суть информационной борьбы, если так можно сказать.

ТРИ ПЕРВЫХ ШАГА

В заключение отметим следующее.

1) Вузам, для подготовки специалистов в соответствии с выбранным профилем подготовки, нужна специализированная учебно-материальная база. Как её создать — вопрос обсуждения с Минобрнауки, но нужны средства. Собственно, по этому пути идут все лучшие учебные заведения мира.

2) Система оплаты работы преподавателей и рейтинговые оценки привлекаемых с рынка, должны быть изменены. Оплату их работы следует осуществлять не по стандартной почасовой ставке, а по договору, «за курс», как это и было ранее, в 90-е годы прошлого века. Но при этом, договорная цена должна быть конкурентоспособна с аналогичными коммерческими курсами.

3) Длительность производственной практики для студентов должна быть существенно увеличена. Один из вариантов — создание в профильных фирмах, выбранных на основании договоров между вузами и фирмами о создании учебных консорциумов, определённого числа временных рабочих мест за счёт государства, коль скоро оно заинтересовано в повышении уровня образования специалистов в области информационной безопасности.



Анатолий АКСАКОВ
председатель Комитета
Государственной Думы РФ
по финансовому рынку

ИТОГИ 2021 ГОДА

ЗАКОНОДАТЕЛЬСТВО В СФЕРЕ ЦИФРОВИЗАЦИИ ФИНАНСОВОГО РЫНКА РАСШИРЯЕТСЯ И УСЛОЖНЯЕТСЯ

В 2021 году было принято несколько важных федеральных законодательных актов, направленных на цифровизацию финансовой сферы. Наиболее активно законодательство развивалось по следующим направлениям.

БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

В 2021 г. продолжилось совершенствование механизмов оказания финансовых услуг с использованием Единой биометрической системы (ЕБС). Возможность подключения к ЕБС помимо банков была предоставлена иным организациям, осуществляющим операции с денежными средствами или иным имуществом, регулирование, контроль и надзор за которыми осуществляет Банк России, — в том числе страховым организациям, микрофинансовым организациям, профессиональным участникам рынка ценных бумаг, НПФ, а также операторам финансовых платформ (маркетплейсам), операторам обмена ЦФА и т.п.

При этом все указанные финансовые организации получили возможность оказывать услуги после идентификации через ЕБС не только физическим, но и юридическим лицам путём идентификации представителя юридического лица, имеющего право действовать от юридического лица без доверенности и являющегося физическим лицом.

В 2021 г. также был осуществлён перевод ЕБС в статус федеральной государственной информационной системы, что должно повысить доверие как пользователей финансовых услуг, так и их поставщиков, финансовых организаций, к указанной системе.

Большую дискуссию вызвала норма, согласно которой банки с 1 января 2022 года должны были обеспечить оказание клиентам финансовых услуг, таких как открытие счетов (вкладов) и выдача кредитов, с использованием биометрии как на своих сайтах, так и в мобильных приложениях для физических лиц.

Поскольку пока ещё не все банки готовы исполнять данную обязанность, срок её вступления в силу был перенесён

Федеральным законом от 30.12.2021 № 441-ФЗ «О внесении изменений в статью 153 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьи 3 и 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации», на 1 сентября 2022 года.

Также на указанную дату перенесено вступление в силу положений, согласно которым владельцы информационных систем, в которых производится обработка биометрических персональных данных для идентификации и аутентификации, должны будут пройти государственную аккредитацию.

Кроме того, согласно Федеральному закону № 441-ФЗ физические лица, имеющие подтверждённую учётную запись в ЕСИА, получили возможность самостоятельно с использованием мобильного телефона и соответствующего программного обеспечения размещать свои биометрические персональные данные в ЕБС. Подтверждение личности в данном случае будет производиться с использованием заграничного паспорта гражданина, содержащего электронный носитель информации с его биометрическими персональными данными. Полагаем, что введение такой возможности повысит популярность ЕБС среди наших граждан и приведёт к росту оказания финансовых услуг с её использованием.

РАЗВИТИЕ ИДЕНТИФИКАЦИИ

В 2021 году в данной сфере было принято два федеральных закона с одинаковым названием «О внесении изменений в статью 7 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма»».

Одним (№ 370-ФЗ от 19.11.2021) устанавливается, что при осуществлении физическим лицом операций по размену банкнот или монет на банкноты или монеты другого номинала либо по замене повреждённых банкнот или монет, не имеющих признаков подделки, на неповреждённые банкноты или монеты на сумму не более 40 тысяч рублей (сумму в иностранной валюте, эквивалентную 40 тысячам рублей)



не производится идентификация физического лица, его представителя, выгодоприобретателя и бенефициарного владельца, а также упрощённая идентификация физического лица. Исключение установлено для случаев, когда у работников организации, осуществляющей операции с денежными средствами, возникают подозрения, что данная операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путём, или финансирования терроризма.

Для вышеуказанных операций на суммы от 40 000 до 100 000 рублей предусматривается упрощённая идентификация физического лица.

Согласно другому (№ 483-ФЗ от 30.12.2021) любым организациям, осуществляющим операции с денежными средствами или иным имуществом, предоставляется право на основании договора поручить кредитной организации помимо проведения упрощённой идентификации или

идентификации клиента, представителя клиента, выгодоприобретателя и бенефициарного владельца также и обновление информации о них.

Кроме того, закрепляется возможность осуществления упрощённой идентификации посредством направления клиентом — физическим лицом номера своего водительского удостоверения.

Также с 15 тысяч до 40 тысяч рублей повышается пороговая сумма, при котором идентификация (упрощённая идентификация) не проводится в отношении операций по приёму страховых премий по договорам ОСАГО и каско.

Всем организациям, осуществляющим операции с денежными средствами или иным имуществом, предоставлено право воспользоваться с согласия клиента сведениями из Единой системы идентификации и аутентификации (ЕСИА) для подтверждения достоверности сведений, полученных ими в ходе идентификации, и для их обновления.

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД В АНТИОТМЫВОЧНОМ ЗАКОНОДАТЕЛЬСТВЕ

Федеральным законом от 11 июня 2021 года № 165-ФЗ «О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» в целях установления основ контроля (надзора) в сфере применения Федерального закона» предусматривается формирование правовых основ для внедрения дистанционных методов мониторинга состояния исполнения требований законодательства Российской Федерации в сфере противодействия легализации (отмыванию) доходов, полученных преступным путём, финансированию терроризма и финансированию распространения оружия массового уничтожения (ПОД/ФТ/ПРОМУ), а также проведения контрольных мероприятий в названной сфере с учётом риск-ориентированного подхода.

При организации контроля (надзора) в сфере ПОД/ФТ/ПРОМУ органами и организациями применяется риск-ориентированный подход, предусматривающий отнесение деятельности организаций, осуществляющих операции с денежными средствами или иным имуществом, индивидуальных предпринимателей, иных лиц к определённому уровню риска несоблюдения требований, установленных Федеральным законом № 115-ФЗ, принимаемыми в соответствии с ним нормативными правовыми актами Российской Федерации и нормативными актами Центрального банка

Российской Федерации, формируемому ими в том числе с учётом результатов национальной оценки рисков, секторальной оценки рисков, дистанционного мониторинга.

Реализация положений закона повысит эффективность контроля (надзора) за выполнением юридическими лицами и индивидуальными предпринимателями, осуществляющими операции с денежными средствами или иным имуществом, законодательства в сфере ПОД/ФТ/ПРОМУ, позволит сконцентрировать проверочную деятельность на субъектах контроля (надзора), имеющих высокие риски нарушения требований законодательства ПОД/ФТ/ПРОМУ, и тем самым будет способствовать снижению административной нагрузки на бизнес в целом.

ПЛАТФОРМА «ЗНАЙ СВОЕГО КЛИЕНТА» (ПЛАТФОРМА «ЗСК»)

Создание указанной платформы предусмотрено Федеральным законом от 21.12.2021 № 423-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», согласно которому с 1 июля 2022 года Банк России будет осуществлять разделение корпоративных банковских клиентов на группы низкого, среднего и высокого риска проведения подозрительных операций на основании ряда критериев, которые установит с учётом, например, сведений о видах и характере деятельности клиентов; операциях по их счетам; их учредителях, участниках и руководителях и т.д.

Далее Банк России будет передавать указанную информацию о распределении клиентов по группам риска банкам через личные кабинеты. Также он сможет разместить эти данные на своём сайте. Состав информации и порядок доступа к ней регулятор определит отдельно своим нормативным актом.

Относить клиентов к группам риска будут и сами банки в рамках внутреннего контроля, при этом учитывая, в какую группу попали клиенты по версии Банка России.

В качестве последствий распределения клиентов по категориям риска в первую очередь необходимо отметить, что клиенту из группы низкого риска нельзя будет отказать в переводе денег российскому юрлицу или индивидуальному предпринимателю из той же группы (так называемый зелёный коридор). Однако, если банк посчитает операции подозрительными, он сможет отказать в переводе и должен будет изменить группу риска клиента.

В отношении клиента из группы среднего или высокого риска банк сможет отказать в открытии счёта, вкладе или депозите, если есть подозрения на ОД/ФТ, а также расторгнуть договор с клиентом, если за год принято минимум два решения об отказе провести операцию.

В конце 2021 года Банк России начал тестирование платформы, которое продлится до конца марта 2022 года. Сейчас к платформе в пилотном режиме подключены 40 банков, а в дальнейшем число участников

В конце 2021 года Банк России начал тестирование платформы «Знай своего клиента», которое продлится до конца марта 2022 года. Сейчас к платформе в пилотном режиме подключены 40 банков, а в дальнейшем число участников может быть увеличено

может быть увеличено. Планируется, что к 1 июля 2022 года информационный сервис станет доступен всем кредитным организациям. Вопрос о возможности расширения субъектного состава участников финансового рынка, для которых доступен сервис платформы Банка России «Знай своего клиента», будет рассматриваться на последующих этапах функционирования платформы.

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ

Федеральным законом от 24.03.2021 № 50-ФЗ «О внесении изменения в статью 3 Федерального закона «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» дата вступления в силу нормы, устанавливающей закрытый перечень способов идентификации заявителей удостоверяющими центрами в целях создания и выдачи сертификатов ключей проверки электронных подписей, перенесена с 1 апреля 2021 года на 1 января 2022 года.

В связи с повышенными требованиями к удостоверяющим центрам для обеспечения надёжности и бесперебойности выполнения ими своих функций, а также требованиями по информационной безопасности данное изменение позволит удостоверяющим центрам качественно подготовить инфраструктуру к предоставлению услуг заявителям.

Данный перенос срока позволит удостоверяющим центрам, выдающим сертификаты ключей проверки электронных подписей, полностью подготовиться к реализации устанавливаемых законодательством механизмов в части создания защищённых каналов и внедрению систем по взаимодействию с клиентами.

Федеральный закон от 30.12.2021 № 443-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» направлен на плавный переход к новому формату использования электронной подписи.

С 1 января 2022 года вступил в действие Федеральный закон № 476-ФЗ, по которому квалифицированные сертификаты должностным лицам органов власти и руководителям юридических лиц, индивидуальным предпринимателям, нотариусам будут выдавать только удостоверяющие центры ФНС, Казначейства и Банка России.

Остальные лица должны будут получать квалифицированные сертификаты в коммерческих удостоверяющих центрах. Причём такие сертификаты не могут содержать описание полномочий владельца. Соответствующие полномочия должны описываться в машиночитаемых доверенностях.

Вместе с тем с учётом необходимости дополнительной подготовки участников рынка к переходу на новый формат взаимодействия с удостоверяющими центрами указанным Федеральным законом устанавливается, что требования о машиночитаемых доверенностях начинают действовать с 1 марта 2022 года.

С этого же момента до конца года устанавливается переходный период, когда можно использовать либо новый режим, когда используется простой квалифицированный

сертификат плюс машиночитаемая доверенность, либо использовать по старому режиму сертификат с указанием в нём полномочий.

Квалифицированные сертификаты, выданные коммерческими аккредитованными удостоверяющими центрами руководителям организаций, индивидуальным предпринимателям до 31 декабря 2021 года включительно, продолжают применяться в течение всего переходного периода.

Окончательный переход на новый способ управления полномочиями посредством машиночитаемых доверенностей должен быть завершён 31 декабря 2022 года.

При этом вступление в силу нормы об исключительной роли удостоверяющих центров ФНС России (для юридических лиц, индивидуальных предпринимателей, нотариусов), Банка России (для кредитных организаций, операторов платёжных систем, некредитных финансовых организаций), Казначейства России (для должностных лиц государственных органов, органов местного самоуправления) остаётся без изменения (с 1 января 2022 года).

РАСШИРЕНИЕ ФУНКЦИОНАЛЬНОСТИ ФИНАНСОВЫХ ПЛАТФОРМ (МАРКЕТПЛЕЙСОВ)

В связи с принятием Федерального закона от 20.07.2020 № 211-ФЗ на финансовом рынке появился новый институт — финансовые платформы — и новые игроки — их операторы. По состоянию на текущий момент в реестре Банка России зарегистрировано 5 финансовых платформ. При этом в настоящее время с использованием финансовых платформ возможно заключение договоров только с физическими лицами.

В целях развития системы совершения финансовых сделок с использованием финансовых платформ в Государственную Думу внесён и 24 марта 2021 года принят в первом чтении проект федерального закона № 1080911-7 «О внесении изменений в отдельные законодательные акты Российской Федерации».

Законопроект направлен на расширение возможностей финансовых платформ: согласно предлагаемым изменениям услуги оператора финансовой платформы станут доступны юридическим лицам и индивидуальным предпринимателям. Кроме того, расширится «продуктовая линейка» финансовых платформ за счёт увеличения перечня случаев, при которых финансовые организации смогут поручать оператору финансовых платформ проведение предусмотренных «противолегализационным» законодательством процедур идентификации клиентов.

Мы рассчитываем на принятие указанного законопроекта в весеннюю сессию 2022 года.

* * *

Работа над развитием законодательства в сфере цифровизации финансового рынка продолжается. Законодательного регулирования, в частности, требуют цифровой рубль, криптоиндустрия, экосистемы, электронные архивы и персональные данные.



Василий ПИСКАРЕВ
председатель Комитета Государственной Думы
по безопасности и противодействию коррупции

В СТОРОНУ БЕЗОПАСНОГО МИРА

ОТ ПРИЗЕМЛЕНИЯ ИТ-ГИГАНТОВ К МЕЖДУНАРОДНОЙ
СИСТЕМЕ РЕГУЛИРОВАНИЯ ИНТЕРНЕТА



1 января вступил в силу так называемый закон о «приземлении» IT-гигантов. Документ обязывает зарубежные IT-компании, аудитория которых насчитывает в России свыше 500 тысяч пользователей, открыть в нашей стране свои полноценные представительства¹. Диалог об открытии таких филиалов ведётся давно, но конкретные результаты появились только сейчас, когда законодательство предусматривает не только обязанность компаний «приземлиться» в России, но и меры принуждения их к этому.

ПОГОДА ЛЁТНАЯ, «ПРИЗЕМЛЕНИЕ» ОБЯЗАТЕЛЬНО СОСТОИТСЯ

Комитет Государственной Думы по безопасности и противодействию коррупции в ходе очных встреч и

¹ Федеральный закон от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» <http://publication.pravo.gov.ru/Document/View/0001202107010014>

онлайн-общения с руководством крупнейших интернет-платформ неоднократно указывал на необходимость открытия ими филиалов в России. И мы неоднократно убедились в том, что наши требования обоснованы. Коммуникация в условиях, когда руководство компании находится в других часовых поясах, где-то за океаном, да и модераторы там же, и при этом имеют слабые представления о российском законодательстве и русском языке, крайне затруднена и малопродуктивна.

Так, в ходе телемоста в октябре минувшего года с участием Марко Панчини, директора YouTube по взаимодействию с органами государственной власти, и Марины Жунич, директора по взаимодействию с органами государственной власти «Google Россия», мы поставили перед ними вопросы как о систематическом удалении противоправного контента, на распространение которого сервисами Google неоднократно указывал Роскомнадзор, так и о применении компанией двойных стандартов в освещении выборов, политической цензуры в информационном пространстве.

Видеовстреча проходила спустя полгода после первого телемоста, итогом которого стала договорённость с компанией об устранении имеющихся нарушений российского законодательства. И срок для «сверки часов» в полгода назначили сами представители Google. Однако за прошедшие месяцы, несмотря на проделанную компанией работу, предъявленные российским регулятором требования в полном объёме реализованы не были.

В частности, по состоянию на начало октября общее количество неудалённого противоправного материала на интернет-ресурсах Google составляло около 2650 материалов (в том числе на сервисе YouTube — около 2500, на иных ресурсах Google — более 150). В свободном доступе продолжали находиться материалы с призывами к суициду, содержащие пропаганду наркотиков, включая рецепты их приготовления и способы употребления, а также ролики, направленные на вовлечение несовершеннолетних в противоправные действия, опасные для их жизни или здоровья (включая рекламу так называемых зацеперов), и откровенно экстремистские материалы. Кроме того, в этом массиве обнаружилось большое количество материалов, содержащих незаконные призывы к массовым мероприятиям и беспорядкам, оскорбление госсимволов, откровенно недостоверную информацию (фейки), а также информацию нежелательных организаций. При этом ряд экстремистских роликов присутствует в свободном доступе в YouTube от 3 до 6 лет. А ведь по российскому законодательству они должны были быть удалены через сутки после обращения Роскомнадзора.

Такое вот, мягко говоря, неспешное поведение компаний в удалении противоправного контента и нежелание следовать нормам российских законов не остались без внимания. Впервые в России в конце прошлого года на Google и Meta² наложили оборотные штрафы размером в несколько миллиардов рублей. Это чёткое свидетельство того, что российские власти от своих требований уважать нашу Конституцию и законы не отступят. Мы в Государственной Думе также внимательно наблюдаем за происходящим и обязательно

² Компания Meta владеет сервисами Facebook, WhatsApp и Instagram



Телемост Комитета Государственной Думы по безопасности и противодействию коррупции с представителями руководства Google и YouTube

проанализируем опыт применения закона о «приземлении». Кроме того, мы продолжим добиваться прекращения блокировки телеканала RT Deutsch на видеохостинге YouTube. Это явное проявление политической цензуры и дискриминации российских СМИ.

Не могу не отметить, что в наступившем 2022 году «лёд всё же тронулся». Крупные IT-компании, которые, несомненно, заинтересованы в присутствии на российском рынке, начали выполнять требования российского законодательства. Первыми открыли личные кабинеты на сайте Роскомнадзора и сделали на своих сайтах формы для обращений граждан России Apple, Viber, Likee, позднее свои личные кабинеты локализовали также Spotify, TikTok и Twitter. При этом Viber уже открыл в России своё официальное представительство. Ожидаем, что в ближайшее время их примеру последуют и остальные компании, которые внесены Роскомнадзором в соответствующий перечень, и осуществят «приземление» на российском правовом поле в полном объёме³.

ЭКСТРЕМИСТСКИЕ МАТЕРИАЛЫ ЗАБЛОКИРУЮТ БЫСТРЕЕ

Перед самым Новым годом Президент России Владимир Путин подписал федеральный закон⁴, который предусматривает оперативную блокировку информации, содержащей

обоснование или оправдание экстремизма и терроризма, а также ложных сообщений о терактах, которые в последнее время массово рассылаются, чтобы посеять панику среди людей и парализовать работу школ, больниц и торговых центров, мешают работе избирательных комиссий.

Считаем принципиально важным как можно быстрее пресекать распространение материалов экстремистской и террористической направленности, так как они ориентированы в первую очередь на молодёжь и преследуют цели радикализации несовершеннолетних. Подростки не обладают в должной мере критическим мышлением, и немало таких случаев, когда они попадают в сети вербовщиков террористических сообществ.

По данным Генеральной прокуратуры, количество преступлений экстремистской направленности растёт. За 11 месяцев 2021 года отмечен рост таких преступлений более чем на 25 %, причём более половины из них совершены с использованием Интернета.

При этом число выявленных фактов публичных призывов к осуществлению террористической деятельности, публичного оправдания терроризма или пропаганды терроризма возросло на 33 % — зарегистрировано 378 таких преступлений.

Ещё одна важная поправка позволяет оперативно блокировать доступ к заведомо ложным сообщениям об актах терроризма. Из-за сообщений о якобы готовящемся теракте эвакуируются сотни людей, закрываются на проверку больницы, школы, магазины, предприниматели терпят убытки. Таких сообщений о ложном минировании объектов социальной инфраструктуры и органов власти Российской Федерации за 2021 год зафиксировано более 4500, и их нужно решительно пресекать, блокируя источники распространения ложной информации. В большинстве своём они поступают с зарубежных электронных сервисов, расположенных в США,

³ В настоящий момент в перечне РКН находится 13 компаний — Google LLC, Apple Distribution, Meta Platforms, Inc., Twitter, Inc., TikTok Pte. Ltd., Telegram Messenger, Inc., Zoom Video Communications, Inc., Likeme Pte. Ltd., Viber Media S.a r.l., Discord, Inc., Pinterest, Inc., Spotify AB, Twitch Interactive Inc: <https://236-fz.rkn.gov.ru/agents/list>

⁴ Федеральный закон от 30.12.2021 № 441-ФЗ «О внесении изменений в статью 15-3 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьи 3 и 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации»»: <http://publication.pravo.gov.ru/Document/View/0001202112300008>



На связи с Государственной Думой директор YouTube по взаимодействию с органами государственной власти в странах Европы, Ближнего Востока и Африки Марко Панчини



Председатель Комитета Государственной Думы по безопасности и противодействию коррупции Василий Пискарев

Канаде, Японии, ФРГ, Нидерландах и ряде других стран, а также с Украины.

На расширенном заседании Комитета Государственной Думы по безопасности и противодействию коррупции в ближайшее время обсудим совместно с представителями ФСБ и МВД России вопрос о том, как работают уже принятые законы, и о необходимости законодательных изменений для противодействия этому явлению. В большинстве случаев ложного минирования мы сталкиваемся с ещё одной формой зарубежного вмешательства с целью дестабилизировать внутривнутриполитическую обстановку в нашей стране, и такие действия должны получать достойный ответ.

ИНТЕРНЕТ НЕ ДОЛЖЕН БЫТЬ ПЛОЩАДКОЙ ДЛЯ КИБЕРВОЙН

Позиция России в сфере регулирования норм поведения в интернет-пространстве принципиально отличается от подхода, которого сегодня придерживаются страны Запада. Мы убеждены, что «глобальная паутина» не может существовать по правилам, диктуемым каким-либо одним государством, или существовать в системе координат, установленных глобальными IT-корпорациями. С учётом уважения суверенитета государств Интернет должен сохранять свою целостность и иметь демократические международные институты управления.

К сожалению, наши западные партнёры систематически пытаются привнести в информационное пространство элементы «цифровой холодной войны», оперируя военными терминами и планируя военные операции в киберпространстве.

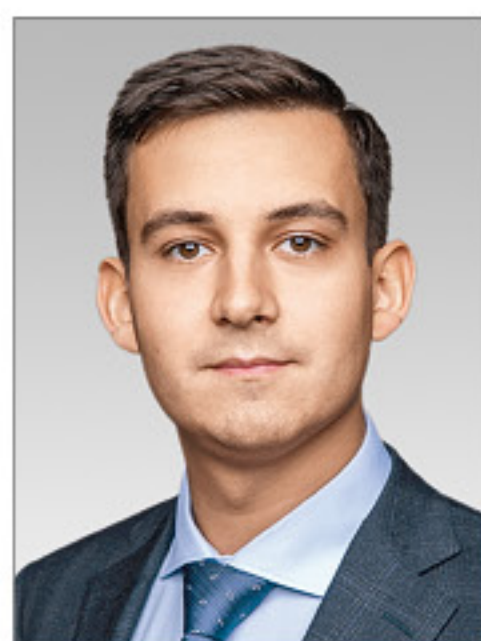
Вот уже много лет наша страна добивается на площадке ООН принятия справедливых решений в сфере международной информационной безопасности. И несомненным достижением следует назвать принятую на условиях консенсуса с участием 108 стран российско-американскую резолюцию Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения

государств в сфере использования информационно-коммуникационных технологий (ИКТ)».

По инициативе нашей страны созданы Рабочая группа ООН открытого состава по вопросам использования ИКТ и самих ИКТ на период 2021–2025 годов, а также Спецкомитет ООН по разработке универсальной международной конвенции по противодействию использованию ИКТ в преступных целях. Важным достижением также является возобновление двустороннего диалога с США в этой сфере. Но, конечно же, наша цель — не переговоры ради переговоров, а достижение конкретно результата. В данном случае — создание международно-правовых основ регулирования информационного пространства для предотвращения конфликтов.

Здесь должны, безусловно, соблюдаться два принципа. С одной стороны — межгосударственное, основанное на равноправном участии управление Интернетом, а с другой — сохранение суверенного права государств на управление его национальными сегментами. В этом плане Россия получает поддержку со стороны наших партнёров по ОДКБ, ШОС и БРИКС. Необходимо расширять взаимодействие между нашими странами, активно используя методы парламентской дипломатии.

При этом хотелось бы сказать ещё об одном, о чём не следует забывать ни при каких обстоятельствах. Современная международная обстановка диктует необходимость рассматривать все варианты развития событий. Поэтому очень важно серьёзно подойти к подготовке квалифицированных специалистов по информационной безопасности, конструкторов и программистов, созданию инфраструктуры по разработке и производству собственной элементной базы и отечественного программного обеспечения. Это сложный путь, но его необходимо пройти. От этого во многом зависит безопасность и надёжность функционирования объектов критической инфраструктуры.



Никита ЛОМОВ
руководитель
аналитического
отдела Ассоциации
ФинТех

ФИНТЕХ, КОТОРЫЙ ВСЁ ИЗМЕНИЛ

2021 год был головокружительным с точки зрения событий в финтех-индустрии. И в этом году мы увидим, насколько широко распахнулись «окна возможностей» для финансового рынка. Откуда ждать перемен и что они нам принесут?

ГОНКА ЦИФРОВЫХ ВАЛЮТ

Цифровые валюты центральных банков (CBDC) стали одной из самых обсуждаемых тем прошлого года. Варианты использования цифровых валют изучают около 80% центральных банков по всему миру, а 40% тестируют их концепции, и Россия не исключение. В этом году планируется провести пилотирование платформы цифрового рубля. На первом этапе будут протестированы эмиссия цифрового рубля, переводы между физлицами и взаимодействие клиента, банка и платформы цифрового рубля.

Какие преимущества даёт введение CBDC?

Снижаются издержки на операции с деньгами, а это значит уменьшение затрат для бизнеса. Финансовые организации смогут развивать для граждан и бизнеса инновационные сервисы на базе цифровых валют, в том числе за счёт применения смарт-контрактов. При этом

будет обеспечен высокий уровень сохранности и безопасности цифровых денег.

ОТКРЫТЫЙ БАНКИНГ. ВРЕМЯ ПРИШЛО

Открытый банкинг может изменить финансовый сектор. С помощью стандартизированных открытых API (программных интерфейсов) финансовые организации могут обмениваться информацией в безопасной и защищённой среде. В 2021 году мы существенно продвинулись в этом направлении. Банк России выпустил шесть рекомендательных стандартов для открытых банковских интерфейсов. На площадке Ассоциации ФинТех действует стенд, на котором можно пройти проверку на соответствие этим стандартам.

Что дальше?

В прошлом году ЦБ сообщил, что планирует определить подход к регулированию открытых API и реализовать необходимые меры по обеспечению обмена данными с их использованием.

Это позволит унифицировать взаимодействие организаций через открытые API. В итоге разработчики получают возможность создавать решения, которые они смогут интегрировать в

приложения, в том числе супераппы различных кредитных организаций или других участников финансового рынка без необходимости внесения существенных модификаций.

Всё это делается, чтобы потребители финансовых услуг получили новые удобные услуги и сервисы. Важно, что в среде открытого банкинга обмен данными происходит только с согласия пользователей.

БЛОКЧЕЙН. ВСЁ СЕРЬЁЗНО

2021 год можно назвать годом активного развития блокчейн-платформ. В сентябре прошлого года председатель Правительства РФ Михаил Мишустин подписал постановление о проведении эксперимента по оформлению электронных закладных на блокчейн-платформе «Мастерчейн». Цель — обеспечить безопасное хранение закладных в электронном формате и ускорить перевод ипотеки в онлайн-формат.

Платформа «Мастерчейн» была разработана Ассоциацией ФинТех путём модификации блокчейн-протокола платформы Ethereum. В конце 2019 года технологию сертифицировала ФСБ на соответствие требованиям криптографической защиты информации. Оператором платформы выступает компания «Системы распределённого реестра».

Использование технологии блокчейн значительно увеличит стабильность и надёжность данных об электронных закладных.

В прошлом году развитие получил и проект блокчейн-платформы ФНС для подтверждения льготных кредитов бизнесу. Сейчас в платформу входит более 200 узлов, к системе подключены более 70 кредитных организаций. Блокчейн позволяет моментально синхронизировать информацию между участниками. Таким образом, скоринг заёмщиков производится за минуты. В 2021 году на базе этой сети был запущен пилотный проект по машиночитаемым доверенностям. В 2022 году планируется реализация новых государственно-частных проектов на базе блокчейна.

ПЛАТЁЖНЫЙ ПЕРЕВОРОТ

За прошедшие несколько лет мы стали практически безналичной страной. Банк России ожидает, что доля безналичных платежей по итогам 2021 года будет не меньше 73%. Обороты растут, а правила игры на рынке задают всё те же платёжные системы. Но совсем скоро всё изменится. В прошлом году Центральный банк объявил о планах по созданию института небанковских поставщиков платёжных услуг (НППУ). Это позволит выйти на рынок новым компаниям.

Сложившаяся при расчётах платёжными картами бизнес-модель (с участием банка-эмитента, банка-эквайера, плательщика и торгово-сервисного предприятия), а также тарифная политика

А ЧТО ДУМАЮТ ЛЮДИ?

Ассоциация ФинТех (АФТ) представила результаты исследования мнения рынка по вопросам развития финансовых технологий на 2021–2023 гг. Документ был подготовлен совместно с международной консалтинговой компанией Accenture.

Исследование включает обзор глобальных трендов, текущий статус развития финансовых технологий в России и взгляд участников рынка на развитие финтеха в ближайшие годы. В ходе исследования были выделены приоритетные направления на 2021–2023 гг. Для подготовки документа были проведены опросы 79 организаций финансового сектора и более 30 глубинных интервью с экспертами и лидерами отрасли, включая руководителей крупнейших игроков рынка, отраслевых ассоциаций и институтов развития.

По результатам опроса был сформирован перечень приоритетных направлений развития финансовых технологий:

- ♦ развитие цифрового профиля для физических и юридических лиц;
- ♦ создание доверенной среды открытых API;
- ♦ расширение доступа к национальной платёжной инфраструктуре (в т. ч. для небанковских игроков);
- ♦ разработка подходов к регулированию экосистем;
- ♦ развитие экспериментальных правовых режимов;

- ♦ актуализация регулирования в области использования данных и обмена ими;

- ♦ цифровизация исполнительного производства;
- ♦ развитие биометрической идентификации;
- ♦ цифровизация процесса ипотечного кредитования;
- ♦ цифровизация торгового финансирования и развитие цифрового факторинга — платформы онлайн-финансирования поставок МСП;

- ♦ создание стандартов для развития блокчейн-сетей;
- ♦ создание единых стандартов и общей инфраструктуры по ДМС для обмена данными между страховыми компаниями и лечебными учреждениями.

— Развитие рынка финансовых технологий идёт опережающими темпами. Проведённое исследование обозначило видение рынка по основным направлениям развития финтеха на ближайшие несколько лет. Для нас было важно представить консолидированное мнение профессионального сообщества. Это поможет сконцентрироваться на движении к общим целям, — прокомментировала гендиректор Ассоциации ФинТех Татьяна Жаркова.

Полная версия исследования доступна по ссылке <https://www.fintechru.org/analytics/>

карточных платёжных систем, с одной стороны, позволяет возмещать издержки банков на развитие инфраструктуры и стимулировать безналичные платежи, с другой — порождает высокие издержки для бизнеса.

Изменение бизнес-модели, когда НФО и нефинансовые организации в статусе НППУ смогут самостоятельно заниматься эквайрингом (обрабатывать операции по картам и онлайн-платежам, обмениваться платёжной информацией с банками-эмитентами), позволит снизить издержки на приём платёжных карт.

В докладе Центрального Банка «Совмещение видов деятельности на финансовом рынке», который представлен для общественных консультаций, говорится, что нефинансовые организации смогут получить статус НППУ при условии включения в реестр Банка России. Для этого должны быть выполнены требования по минимальной стоимости чистых активов и к ПОД/ФТ, а должностные лица таких организаций должны соответствовать квалификационным требованиям и требованиям к деловой репутации.

К этому стоит добавить, что Система быстрых платежей быстро завоёвывает рынок не только как способ перевода наличных, но и как средство оплаты. Пользоваться ей могут все субъекты бизнеса независимо от размера и сферы

деятельности. Для приёма платежей СБП можно применять практически везде. Одно из главных преимуществ — меньший размер комиссий по сравнению с классическим эквайрингом.

По данным Центрального банка, в планах по развитию СБП предоставить гражданам возможность совершать платежи в пользу государственных органов (сервис С2G) и, наоборот, получать выплаты из бюджета (сервис G2C). Кроме того, планируется пилотный проект по перечислению зарплат с использованием СБП.

НОВЫЕ ИГРОКИ — НОВЫЕ ЭКОСИСТЕМЫ?

Этого ждали, это обсуждали, и в 2021 году это произошло. На финансовый рынок пришли ретейлеры и бигтехи. «Яндекс» приобрёл банк «Акрополь» и переименовал его в «Яндекс.Банк». С помощью кредитной организации ИТ-компания планирует создавать финансовые продукты для пользователей и партнёров своих сервисов. Помимо «Яндекс.Банка» в 2021 году появились «Озон Банк» и «Вайлдберриз-банк». Онлайн-ретейлеры намерены идти по тому же пути — начать с финансового обслуживания своих клиентов и поставщиков.

В этом году можно будет наблюдать интеграцию финансовых и нефинансовых сервисов на онлайн-платформах и развитие экосистем.

СТЕНД И ПОРТАЛ ОТКРЫТЫХ API

Для обеспечения безопасности использования открытых API в России Ассоциация ФинТех запустила стенд, на котором банки и финтех-компании проходят проверки на соответствие стандартам Банка России. На информационном портале <https://openbankingrussia.ru/> доступны сведения о рекомендательных стандартах и порядке подключения к сертификационному стенду.

Первыми проверки на стенде прошли «Точка» и Промсвязьбанк. Ещё ряд финансовых организаций находятся на этапе подключения. Первым сервисом, где будут

использоваться открытые API, станет возможность обмена информацией по счетам юридических лиц между банками. Благодаря этому при оформлении кредита компаниям не нужно будет предоставлять в банк-кредитор бумажные выписки по счетам из других банков; достаточно дать согласие на передачу этих сведений в электронном виде банку-кредитору. При этом участники используют единые стандарты открытых API и присоединяются к единым правилам, без необходимости заключения дополнительных договоров друг с другом.

ГАЗПРОМБАНК — ИПОТЕКА — «МАСТЕРЧЕЙН»

В рамках проекта по цифровизации ипотечных сделок Газпромбанк перевёл выпуск закладных на блокчейн-платформу «Мастерчейн», разработанную Ассоциацией ФинТех. Использование «Мастерчейн» позволит отказаться от бумажного документооборота и выпускать закладные в электронном виде. В результате время на выдачу закладной по ипотеке сокращается с 9 дней до одного. Электронная закладная является аналогом бумажной.

Переход на электронные закладные — один из ключевых этапов, необходимых для перехода к оформлению ипотеки в полностью цифровом формате. На сегодня к сервису для выпуска электронных закладных на «Мастерчейн» подключены полтора десятка игроков рынка, в том числе крупные банки. «Мастерчейн» позволяет обеспечить наивысшую безопасность учёта закладных. Платформа прошла сертификацию на применение российских СКЗИ.

ПОСТРОЕНИЕ ВНУТРЕННЕГО SOC

ПЛЮСЫ, МИНУСЫ, ПОДВОДНЫЕ КАМНИ

7–8 декабря в Москве состоялось одно из главных событий года в сфере российской информационной безопасности — SOC-Форум 2021 «Практика противодействия кибератакам и построения центров мониторинга ИБ». Подробный отчёт о нём читайте на стр. 62. А тут, в качестве знакомства с интересным и, надеемся, полезным опытом, публикуем один из докладов, прозвучавших на Форуме¹.

НАЧАЛО

Мы приступили к построению внутреннего SOC в 2018 году, основной целью ставили перед собой создать такую систему мониторинга, чтобы мы первыми узнавали, какие события в рамках информационной безопасности происходят в инфраструктуре банка, и могли незамедлительно реагировать на инциденты.

У нас на тот момент была сформирована команда, которая умела строить IT-инфраструктуру и поддерживать её. Кроме того, у нас был SIRT с талантливыми специалистами.

ЦЕЛИ И ЗАДАЧИ

Далее мы сформулировали первоочередные задачи, которые перед нами стояли (рис. 1).

Не буду детально останавливаться на каждой задаче, думаю, аудитория понимает, о чём идёт речь, но хотел бы обратить внимание на то, что у нас есть пул дочерних компаний, которые тоже необходимо было включить в контур мониторинга, предложив им ту же сервисную модель, которая работает внутри МКБ.

ПОДГОТОВКА К ПРОЕКТУ

С чего мы начали подготовку к проекту? Во-первых, пригласили в команду высококлассного архитектора, его задачей было спроектировать SOC в части технологий и придать ему те контуры, которые он сейчас имеет. В рамках подготовки также был определён руководитель SOC, давно работающий в банке и понимающий многие происходящие процессы. Во-вторых, мы произвели тщательный расчёт серверных мощностей, затем создали архитектуру и достаточно кропотливо подобрали ПО, ставшее основой SOC.

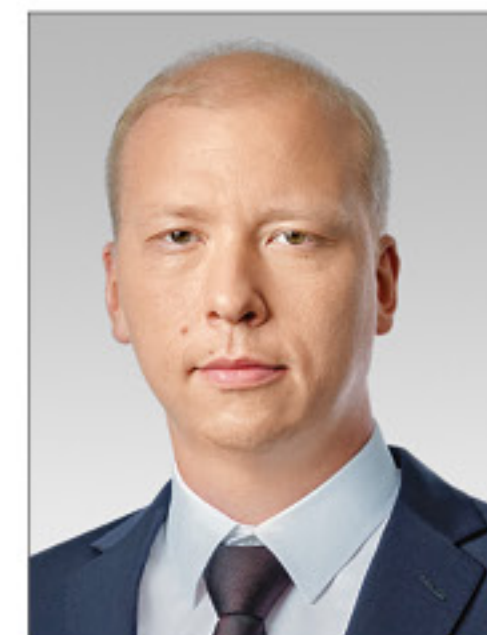
Надо сказать, нам даже удалось сэкономить на ПО, поскольку мы отказались от очень дорогой SIEM-системы, приобретённой банком ранее.

И самое главное — это грамотный расчёт HR, потому что все мы прекрасно знаем, что Security Operation Center — это люди, технологии и процессы. И люди — это наиболее важная часть.

ОБОСНОВАНИЕ ПРОЕКТА

В рамках подготовки к запуску своего SOC мы, естественно, сравнивали его предполагаемую эффективность с коммерческими SOC. Мы очень плотно поработали с «Ангарой», «Бизоном», «Джет» и другими компаниями. Работали честно, у нас не было намерения любой ценой сделать всё самостоятельно, мы были готовы привлечь и внешние SOC. В итоге в сравнении с самым бюджетным предложением у нас стоимость владения SOC за 4 года получилась ниже на 40 процентов.

Во-первых, мы оценили все риски, в том числе остаточные. Мы оценили их количественно, и это стало своеобразным экономическим базисом для утверждения проекта. Во-вторых,



Вячеслав КАСИМОВ
директор
департамента
информационной
безопасности
Московского
кредитного банка
(МКБ)

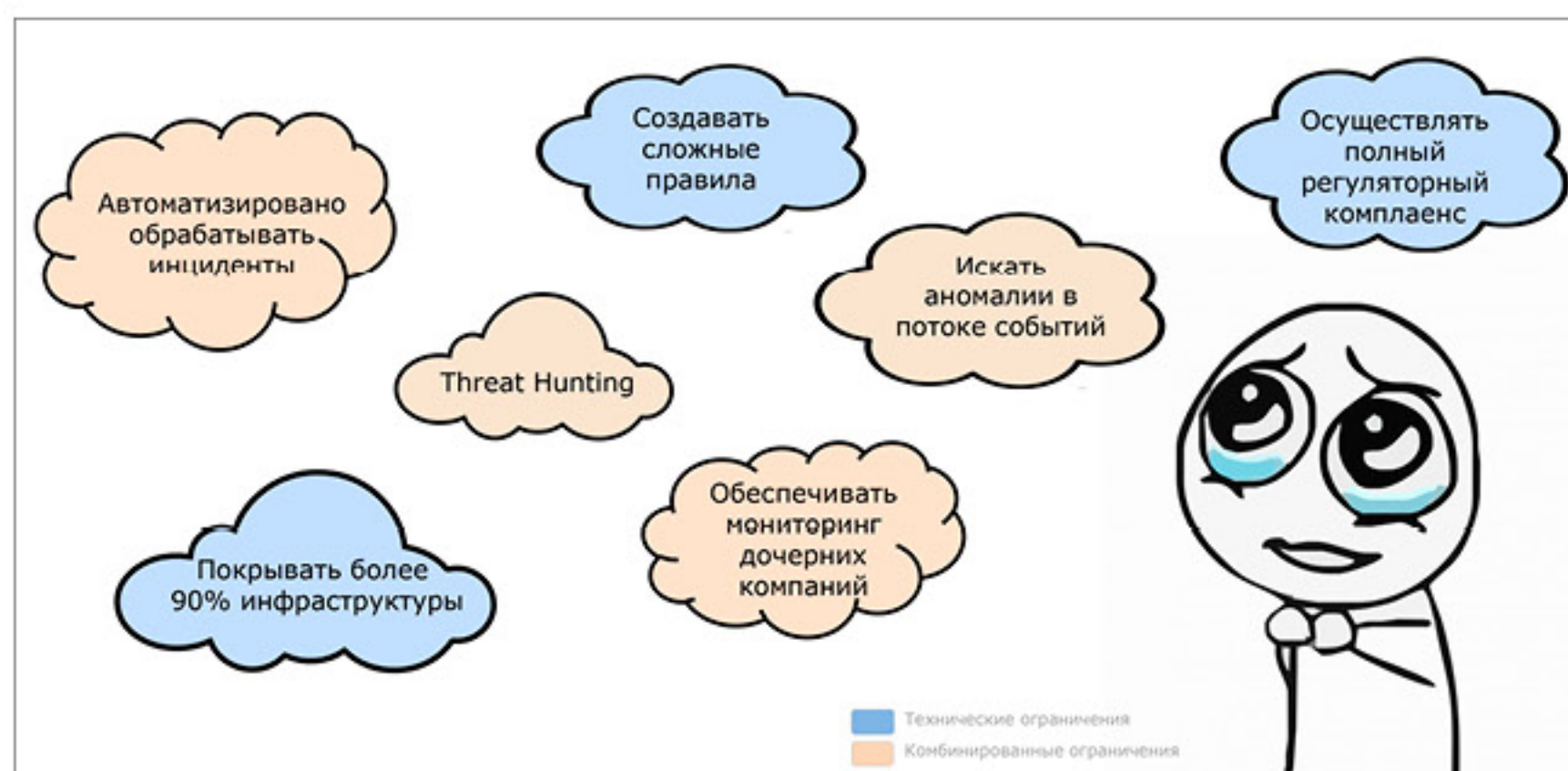


Рисунок 1. «Цели и задачи, которые мы перед собой поставили»

¹ Доклад также опубликован на портале НКЦКИ <https://safe-surf.ru/article/>

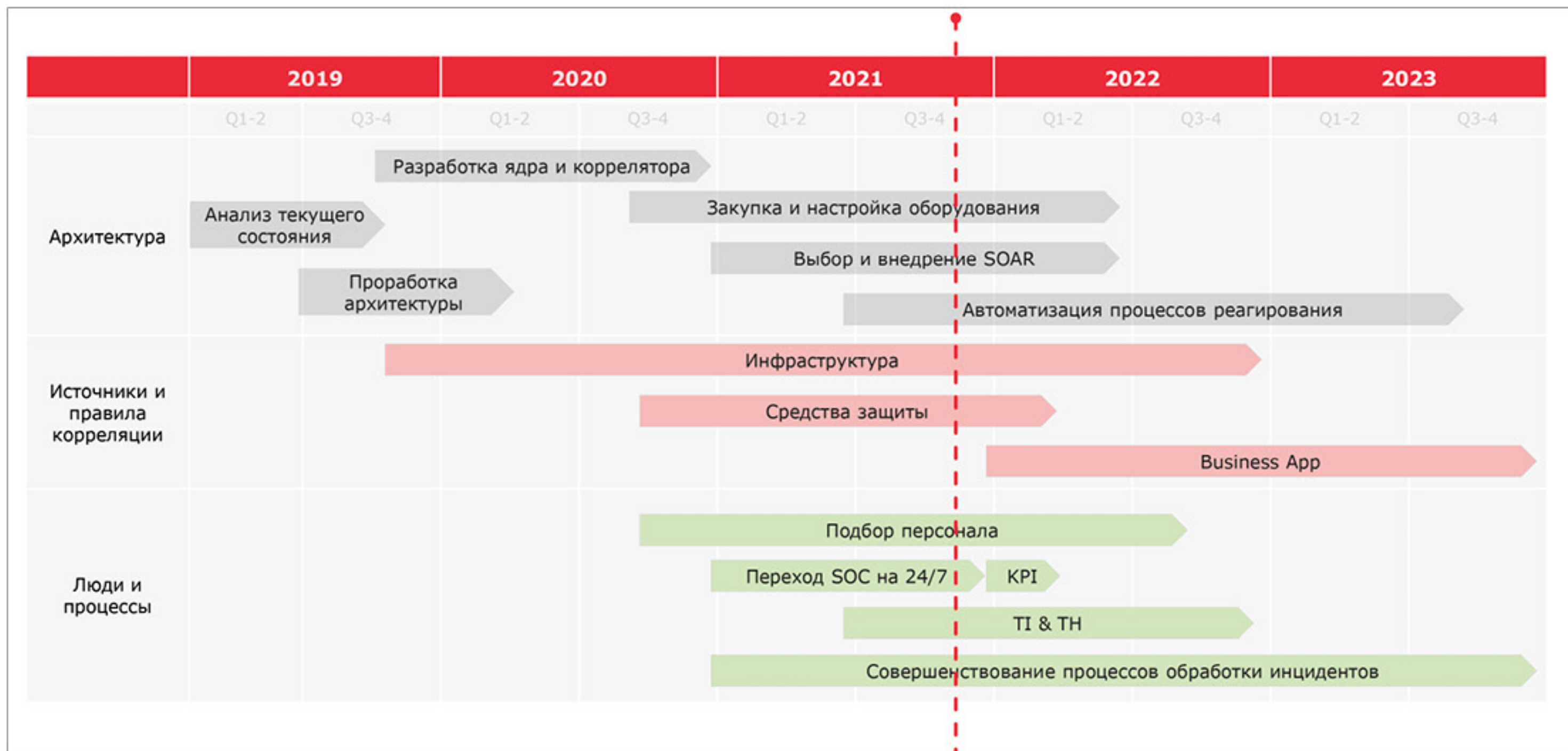


Рисунок 2. «Дальше мы создали план реализации проекта, его дорожную карту»

мы провели детальный анализ как рынка SOC, так и банковского рынка в части мониторинга и реагирования на инциденты: мы изучили, как коллеги из крупнейших банков подходят к решению проблемы. В-третьих, мы подготовили очень точный TCO. Стоимость владения мы показали правлению, чтобы бизнес четко понимал, что сколько стоит и что он получает за обозначенный бюджет.

ПЛАН РЕАЛИЗАЦИИ

Дальше мы создали план реализации проекта, его дорожную карту (рис. 2). Тут важно отметить, что работы по созданию инфраструктуры заняли достаточно большое количество времени. В план вошли не только работы по подключению всех инфраструктурных элементов, но и

создание свода правил по реагированию на события. Например, применительно к операционным системам, правила для Windows мы сейчас перепишем, используя MITRE и другие признанные ИБ-сообществом практики. У нас их получается порядка 130, это довольно много, все их нужно смотреть, имплементировать, выверять, тестировать. Поэтому если вам кто-то скажет, что справился за три месяца, то будьте уверены: либо речь идет об очень маленькой и гомогенной инфраструктуре, либо это неправда.

ИСПОЛЬЗУЕМЫЕ ТЕХНОЛОГИИ

Мы купили большой объем оборудования, в результате получили 336 ядер, 3 терабайта оперативной памяти и около 100 терабайт дисковой подсистемы. Но чтобы завершить задуманную архитектуру, нам предстоит расширить мощности, в первом полугодии 2022 года мы ожидаем очередную крупную поставку «железа». Важная часть работы SOC — предварительная обработка событий. Это позволяет снизить нагрузку на ядро SOC и сделать, насколько это возможно, распределенным прикладной функционал. Мы сделали очереди на базе Kafka, и, соответственно, те инциденты, которые возникают, обрабатываются с помощью Kafka, потом у нас происходит обогащение, затем сравнение и итоговое формирование инцидента. В основном мы сознательно используем open-source либо собственную разработку на Python. Это снимает с нас дополнительные экономические ограничения для перехода на более современные технологии.

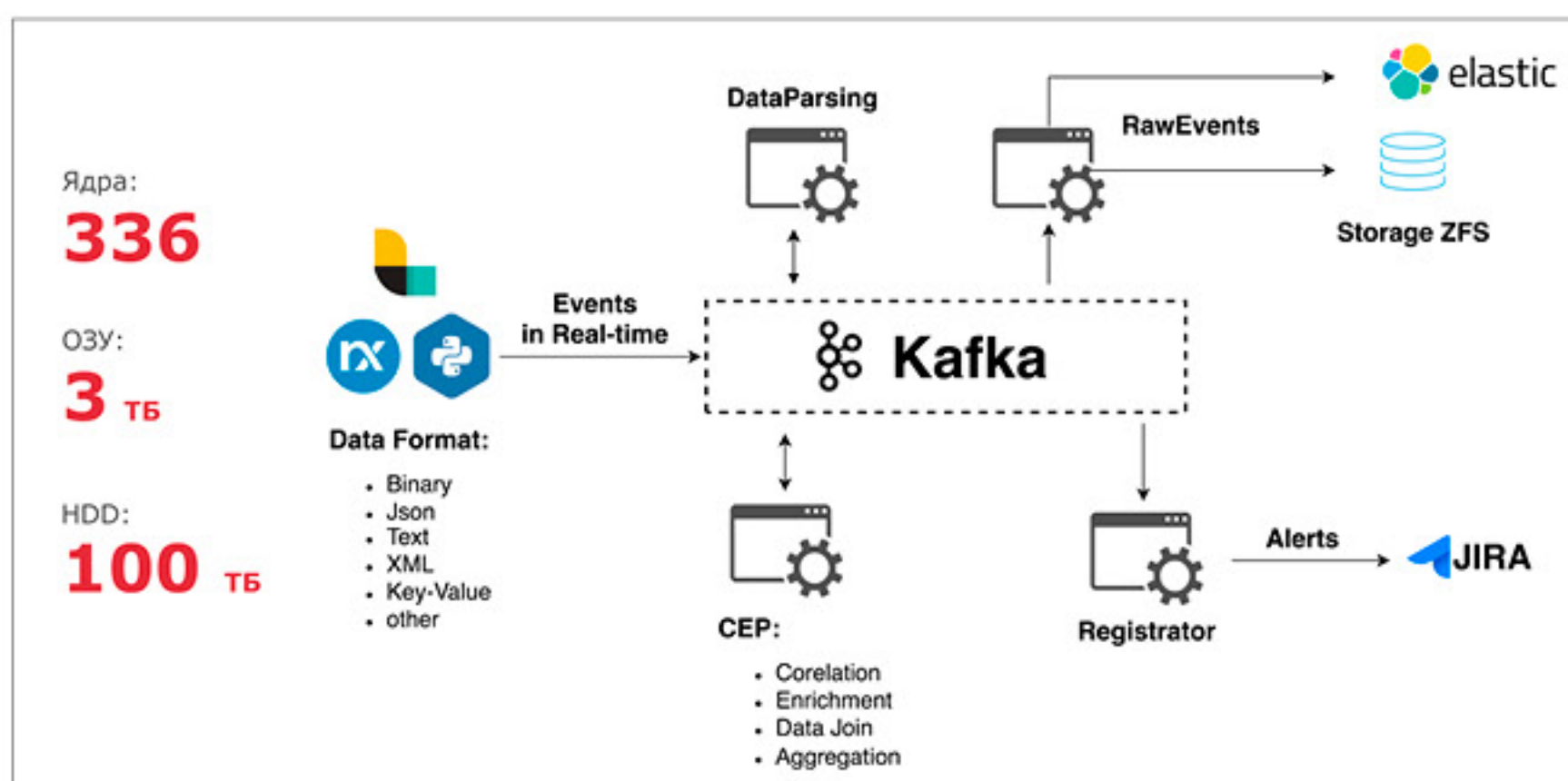


Рисунок 3. Используемые технологии. «Мы купили большой объем оборудования, в результате получили 336 ядер, 3 терабайта оперативной памяти и около 100 терабайт дисковой подсистемы»

ПЛЮСЫ, МИНУСЫ, ПОДВОДНЫЕ КАМНИ

Теперь, собственно, про плюсы-минусы и подводные камни (рис. 8). Какие плюсы?

Стоимость — это очевидно, потому что 40 процентов стоимости владения по сравнению с коммерческими SOC — впечатляющий показатель.

Скорость реагирования. Мы точно реагируем быстрее, потому что скорость реагирования тесно взаимосвязана с другим свойством — управляемостью. А управляемость у нас, понятно, намного выше. Я всегда могу прийти и сказать: «Ребят, давайте ту или иную процедуру поправим и сделаем лучше». В сторонний SOC я, наверное, тоже могу внести правки и усовершенствования, но в рамках соответствующего договора, и совершенно точно речь пойдёт о месяцах или годах и о модификации дорожной карты организации. С учётом того, что у стороннего SOC клиентов много, индивидуальные процедуры могут иметь место, но не думаю, что на постоянной основе.

Какие минусы? Скорость реализации. В общем-то, мы сразу настраивались на то, что этот проект займёт несколько лет. Сейчас мы создали базис, который умеет всё. Этот год мы посвятили очень важным вещам, я бы сказал, основным: написанию ядра, подключению ключевой инфраструктуры, созданию и отладке коллекторов и т.д. То, что в ходе работы возникло 117 правил, не было запланированным, потому что акцент на правила у нас выпадал на 2022 год. Безусловно, скорость реализации в коммерческом SOC была бы выше, даже несмотря на договорные процедуры и на то, что инфраструктуру так же нужно было бы подключать.

Огромный минус — это поиск персонала. У нас есть несколько классных специалистов, которые двигают процесс. Но хантинг на рынке таких единичных специалистов — это на

самом деле стоп-фактор. Их на рынке практически и нет. Нужно владеть ситуацией, знать людей, контакты, чтобы находить тех, кто умеет и может. Но и этого недостаточно. Чтобы людей привлечь, нужны всяческие плюшки, и не только материальные. Ведь эти специалисты, по-своему звёзды, должны захотеть к вам прийти, сказать: «О! Да тут прикольно будет работать!» И вот эти ключевые фигуры являются главным подводным камнем, так как в один прекрасный момент такой человек может встать и пойти своим светлым путём. Соответственно, надо заранее создавать кадровый резерв, готовить аналогичных по уровню специалистов.

Другой подводный камень — понимание ответственными лицами, зачем и какой нужен SOC. CISO должен отчётливо представлять, что он получит в результате и в каком виде. Если такого представления нет, то и полноценного результата не будет, независимо от того, идёт речь о внутреннем или коммерческом SOC. Если у руководителя нет картинки в голове, то, скорее всего, системообразующий договор получится нежизнеспособным как минимум в первый год работы.

Кроме того, безопасник обязан быть толмачом, переводчиком. Это значит, что я должен постоянно переводить с нашего технического уругвайского на бизнесовый парагвайский. Когда такой перевод происходит, бизнес начинает понимать, о чём идёт речь, становится адекватным и выделяет деньги на то, что, как оказывается, для него полезно.

Ну, и вера в свои силы. Да, это тоже важно, потому что где-то на полпути случается, что какие-то процессы идут медленно, что-то перестаёт получаться, или снова приходится переписывать ядро и т.п. Это демотивирует, и всегда нужно находить какие-то положительные моменты в том, что реализуется. Вот на этом пожелании каждому и всем верить в свои силы я и закончу.

Рисунок 8. Плюсы, минусы, подводные камни

 • Стоимость • Скорость реагирования • Управляемость	 • Скорость реализации • Поиск персонала	 • Ключевые фигуры • Четкое понимание желаемого результата • Умение быть толмачом • Дружба с экономикой, excel, powerpoint • Вера в свои силы
---	---	--



Kaspersky Unified Monitoring and Analysis Platform

Центральный элемент единой платформы безопасности

- Мониторинг и анализ инцидентов ИБ
- Поточковая корреляция в режиме реального времени
- Автоматическое обогащение данными об угрозах
- Масштабируемая архитектура и низкие системные требования
- Тесная интеграция с решениями «Лаборатории Касперского» и сторонних производителей
- Обеспечение соответствия законодательству в сфере безопасности объектов КИИ

kaspersky АКТИВИРУЙ
БУДУЩЕЕ

kaspersky.ru/enterprise

ДиалОгНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru



Иван ЯНСОН
бизнес-партнёр
по информационной
безопасности,
Департамент
безопасности
ПАО «Сбербанк
России», кандидат
физико-
математических наук



Николай БОГДАНОВ
заместитель
генерального
директора
АО «Деловая среда»

РБидос расправляет плечи

РЕЗУЛЬТАТЫ И ПЕРСПЕКТИВЫ ЭКСПЕРИМЕНТОВ ПО ДИСТАНЦИОННОЙ РЕГИСТРАЦИИ БИЗНЕСА И ОТКРЫТИЮ СЧЕТОВ

Сбербанк совместно с рядом госструктур реализовал эксперименты по безопасной дистанционной регистрации юридических лиц и индивидуальных предпринимателей, а также удалённому открытию расчётных счетов. По результатам экспериментов был создан сервис «Регистрация бизнеса и дистанционное открытие счёта» (РБидос), с помощью которого в 2020–2021 годах зарегистрировано 92 и 122 тыс. юридических лиц и ИП. Это соответственно 11 и 13 % от общего количества регистраций в Российской Федерации в указанные годы.

Основным элементом сервиса РБидос является применение специализированной защищённой автоматизированной системы (СЗАС), предназначенной для дистанционного формирования и применения квалифицированной электронной подписи.

В статье речь пойдёт о данном сервисе, в частности, о применении технологии мобильной электронной подписи при регистрации бизнеса и открытии счетов, а также о наших предложениях по развитию данной технологии для повышения удобства работы российского бизнеса.

ИСТОРИЯ ВОПРОСА

Традиционно в России регистрация нового бизнеса и открытие расчётного счёта были связаны с рядом обязательных и обременительных процедур. По комментариям предпринимателей, процесс был максимально бюрократизированным и сложным:

- ◆ непонятно, какой пакет документов необходим для регистрации ИП, ООО, для открытия счёта в банке, как правильно его заполнить;
- ◆ сложная процедура формирования квалифицированной электронной подписи (КЭП) и подписания документов;

- ◆ обязательные посещения налоговой инспекции, банка, удостоверяющего центра;

- ◆ оплата госпошлины, дополнительные траты на помощь для сбора и формирования документов.

В итоге часть начинающих бизнесменов не доходила до регистрации своего бизнеса.

По инициативе Правительства Российской Федерации в 2016–2020 гг. были проведены два эксперимента¹ по созданию и совершенствованию применения технологии электронной подписи для упрощения процедур государственной регистрации юридических лиц и ИП, и открытия им банковских счетов.

Первый эксперимент был направлен на создание, тестирование и сертификацию новых технологий. В рамках второго эксперимента новая технология была доработана и выведена на рынок в составе доступного сервиса.

РЕЗУЛЬТАТЫ ПЕРВОГО ЭКСПЕРИМЕНТА

В ходе проведения первого эксперимента были созданы и сертифицированы следующие инновационные технологии:

¹ Первый эксперимент: Постановление Правительства РФ от 29 октября 2016 г. № 1104 «О проведении в 2016–2018 годах эксперимента в целях обеспечения направления электронных документов для государственной регистрации юридических лиц и индивидуальных предпринимателей и открытия им счетов в кредитных организациях с использованием специализированной защищённой автоматизированной системы, предназначенной для централизованного создания и хранения ключей усиленной квалифицированной электронной подписи, а также их дистанционного применения владельцами квалифицированных сертификатов ключа проверки электронной подписи». Второй эксперимент: Постановление Правительства РФ от 8 ноября 2019 года № 1427 «О проведении эксперимента по совершенствованию применения технологии электронной подписи».

♦ после вынесения ФНС России положительного решения о регистрации бизнеса подписать усиленной квалифицированной ЭП в мобильном приложении электронные документы на открытие банковского счёта и направить их в банк.

Ключевым компонентом сервиса РБиДОС и одним из основных результатов эксперимента стало создание и сертификация мобильной электронной подписи — мобильного приложения IDPoint. По сути, это средство криптографической защиты информации в мобильном исполнении, представляющее собой клиентское приложение, функционирующее на мобильных устройствах в составе СЗАС и позволяющее формировать, хранить и применять ключи квалифицированной ЭП.

IDPoint поддерживает российские криптографические стандарты серии ГОСТ Р, взаимодействуют с серверной частью по соединению, защищённому двусторонним TLS-ГОСТ. По результатам успешно завершившихся сертификационных испытаний от ФСБ России получены подтверждения соответствия СКЗИ IDPoint for iOS и IDPoint for Android классу КС1 требований к СКЗИ и средствам ЭП. Далее на мобильное приложение IDPoint были получены сертификаты ФСБ России СФ/114-3774 от 22.11.2019 (на iOS) и СФ/114-3893 от 31.08.2020 (на Android).

Ключи ЭП создаются, хранятся и используются в приложении IDPoint, установленном на пользовательском мобильном устройстве. Для шифрования ключей ЭП используется симметричный ключ шифрования (ключ защиты ключа ЭП), который хранится в СЗАС, в HSM, также в зашифрованном виде. Для шифрования используется парольный ключ, формируемый из пользовательского пароля. Для того чтобы подписать электронный документ на пользовательском устройстве, между мобильным приложением и СЗАС устанавливается защищённое с использованием двухстороннего ГОСТ-TLS соединение. Далее контейнер с ключом защиты передаётся на мобильное устройство, все ключи последовательно расшифровываются, а после использования ключ защиты уничтожается из памяти устройства.

Доступ к сервису может осуществляться путём интеграции информационной системы заказчика с СЗАС. Взаимодействие осуществляется по защищённому каналу с использованием криптографических средств защиты канала связи, сертифицированных ФСБ России.

Установление личности с целью выдачи квалифицированных сертификатов может осуществляться как очно, так и дистанционно с

использованием загранпаспорта нового поколения. Эта технология была опробована в рамках проекта и вошла в закон «Об электронной подписи» в качестве одной из основных технологий дистанционной идентификации. За время проведения экспериментов было отмечено, что эта технология является не менее безопасной, чем традиционная «очная».

Для дистанционной идентификации заявителей с использованием загранпаспортов нового поколения при выдаче квалифицированных сертификатов ключей проверки ЭП применяется сервис проверки паспортно-визовых документов нового поколения (ПВДПН), входящий в состав СЗАС и размещённый на мощностях ФГБУ НИИ «Восход». При проведении дистанционной идентификации по загранпаспорту нового поколения мобильное приложение и СЗАС обеспечивают установление защищённого соединения по протоколу Basic Access Control (BAC) и получение с микрочипа, встроенного в загранпаспорт, персональных данных владельца загранпаспорта. После этого данные, полученные из документа, проверяются на целостность и соответствие данным заявителя, и в результате принимается решение о выдаче сертификата квалифицированной ЭП.

СЗАС представляет собой автоматизированную систему, обеспечивающую регистрацию пользователей, сопровождение процессов выдачи и применения квалифицированных сертификатов, а также содержит в себе бизнес-сценарии работы пользователей. Состав СЗАС и схему взаимодействия компонентов СЗАС между собой можно увидеть на рисунке 2.

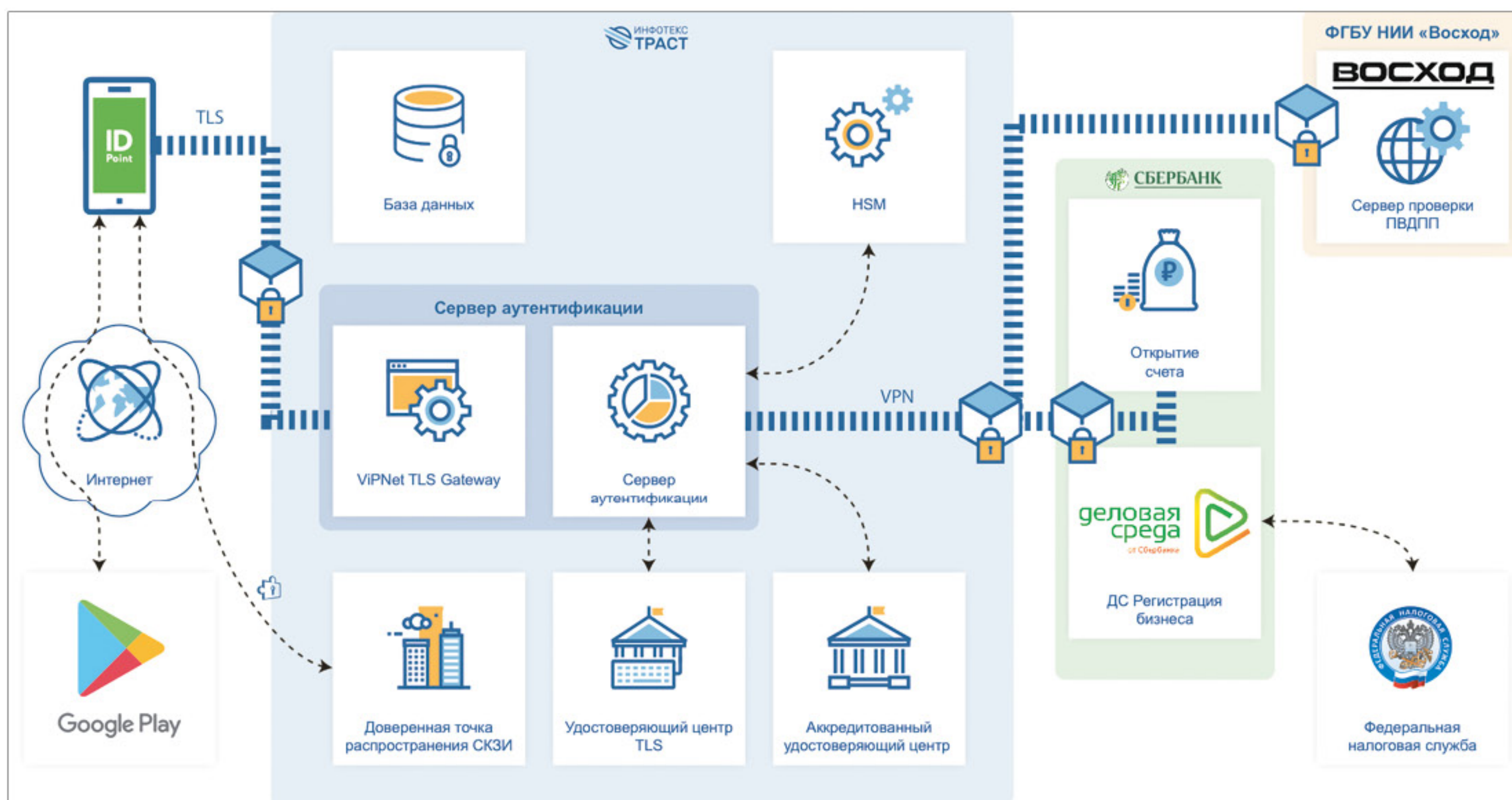
В состав СЗАС входят следующие основные компоненты и сервисы:

♦ основной исполняемый модуль сервера аутентификации (СА СЗАС) — предоставляет API для мобильного приложения IDPoint и внешних информационных систем, обеспечивает выполнение бизнес-сценариев использования СЗАС;

♦ IDPoint — сертифицированное мобильное приложение, входящее в состав СЗАС, предназначенное для создания и хранения ключей усиленной КЭП и их дистанционного применения владельцами квалифицированных сертификатов;

♦ HSM для ключей защиты — ПАК VipNet HSM — защищённое хранилище зашифрованных на пароле клиента ключей защиты ключей формирования ЭП;

♦ TLS Gateway — ПАК TLS Gateway КСЗ — узел, терминирующий TLS-соединения с криптографией согласно ГОСТ с односторонней и двусторонней аутентификацией. Канал от мобильного приложения IDPoint до СЗАС



защищается по протоколу TLS с односторонней и двусторонней аутентификацией и криптографией согласно ГОСТ. Канал TLS с двусторонней аутентификацией terminates на TLS Gateway;

- ♦ ViPNet Coordinator — узел, обеспечивающий безопасную передачу данных между сегментами сети.

- ♦ сервис SMS-рассылок — сервис, обеспечивающий доставку клиенту SMS-сообщений с уникальным кодом клиента для регистрации в мобильном приложении IDPoint;

- ♦ сервис взаимодействия с HSM — обеспечивает передачу на хранение в HSM симметричного ключа защиты КЭП клиента и его получение для целевого использования;

- ♦ сервис взаимодействия с УЦ — обеспечивает взаимодействие с УЦ в рамках выпуска сертификатов электронной подписи клиента;

- ♦ сервис проверки ЭП ФБУ НИИ «Восход» — сервер проверки корректности данных, полученных от чипа ПВДНП; сервис функционирует на вычислительных мощностях ФБУ НИИ «Восход»;

- ♦ УЦ выпуска квалифицированных сертификатов — ПAK ViPNet УЦ КСЗ — удостоверяющий центр, обеспечивающий выпуск квалифицированных сертификатов клиентов;

- ♦ УЦ выпуска сертификатов аутентификации — ПAK ViPNet УЦ КСЗ — удостоверяющий центр, обеспечивающий выпуск сертификатов СА СЗАС и сертификатов аутентификации клиентов.

В ходе практического использования сервиса РБидОС и СЗАС было необходимо осуществить оценку его удобства и качества работы, а также возможность оптимизации клиентского пути при реализации деловых процессов. В этой связи было выпущено Постановление Правительства Российской Федерации № 1427 от 8 ноября 2019 г., целью которого являлось совершенствование применения разработанных ранее технологий электронной подписи и сервиса РБидОС.

РЕЗУЛЬТАТЫ ВТОРОГО ЭКСПЕРИМЕНТА

На текущий момент Сбербанк в рамках своего участия в экспериментах обеспечил с начала 2019 года регистрацию с помощью сервиса более 250 тыс. юридических лиц и индивидуальных предпринимателей, из которых более 15 тыс. зарегистрировались дистанционно, «не выходя из дома», с помощью технологии ПВДНП. За время эксперимента открыто более 200 тыс. банковских счетов.

На рисунках 3 и 4 можно увидеть, как увеличивалось число регистраций бизнеса и открытых счетов через РБидОС.

Отмечается и положительное влияние созданного Сбербанком сервиса РБидОС на выполнение государственной задачи регистрации бизнеса во время пандемии: сервис РБидОС позволил минимизировать социальные контакты предпринимателей в процессе регистрации. Во время «первой волны» пандемии процент

Рисунок 2. Схема взаимодействия компонентов СЗАС

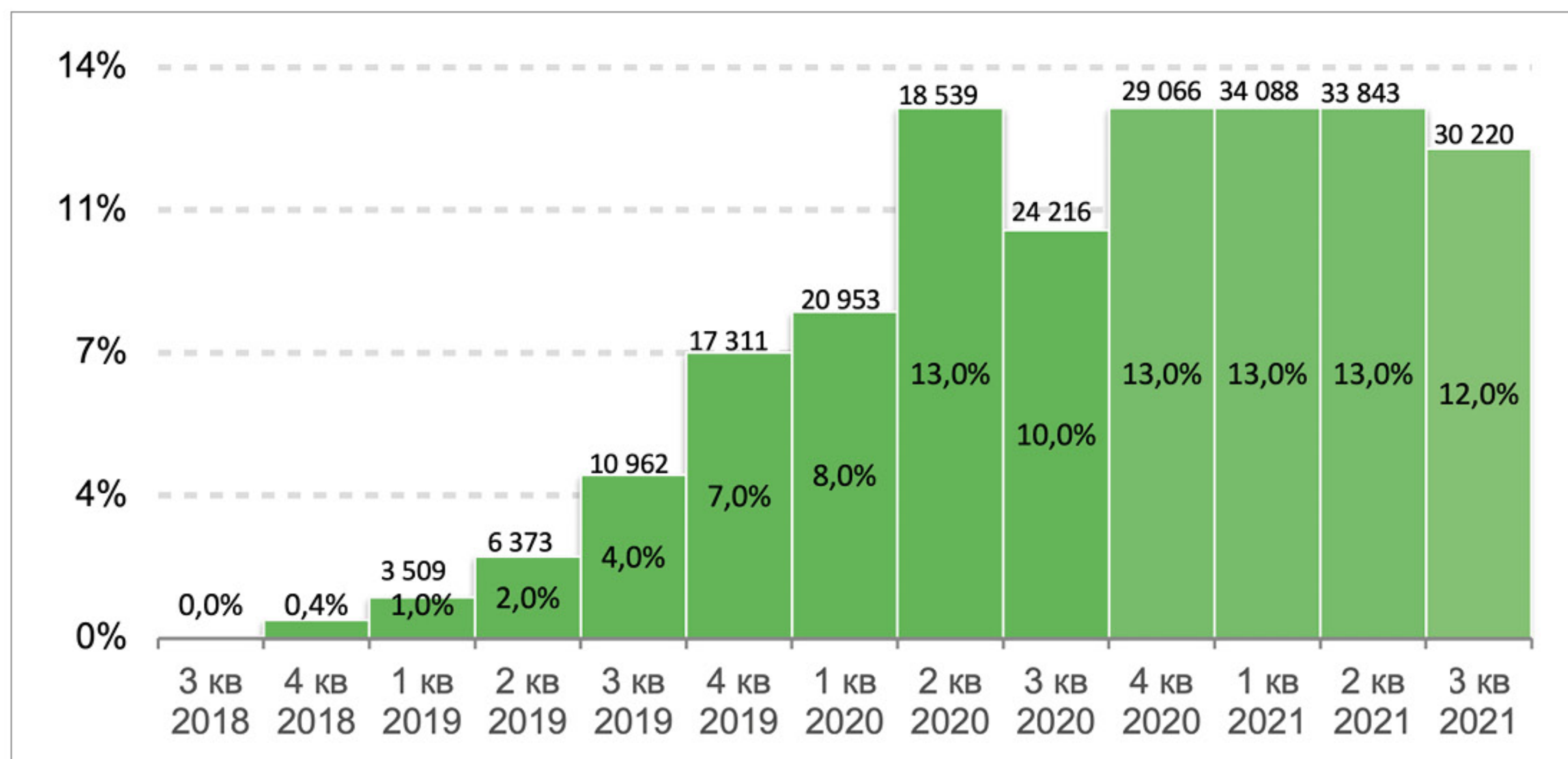


Рисунок 3. Количество бизнесов, зарегистрированных через РБидОС (по данным на конец III кв. 2021)

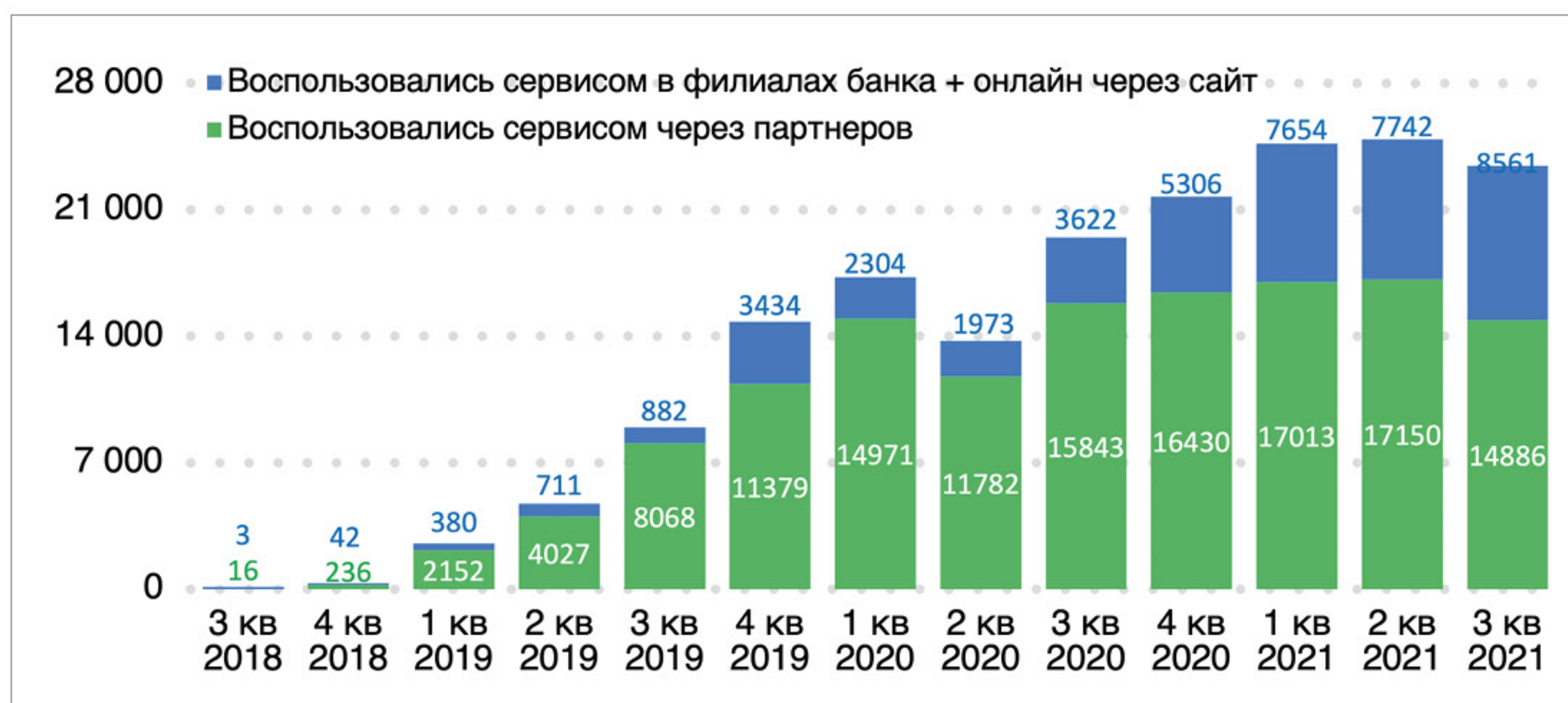


Рисунок 4. Количество счетов, открытых через сервис РБидОС (по данным на конец III кв. 2021)

регистраций через РБидОС увеличился почти вдвое, с 8% в первом квартале 2020 года до 13% во втором квартале 2020 года, достигнув 14–15% в апреле-мае 2020 года.

При этом примерное время, затрачиваемое на взаимодействие гражданина с сервисом РБидОС для регистрации бизнеса и открытия счёта, составляет порядка 45 минут без учёта срока проверки заявки и принятия решения регистрирующим органом. В процессе эксплуатации было также проведено исследование пользовательского опыта клиентов и

рассчитан индекс потребительской лояльности (Net Promoter Score, NPS), который за 2019 год составил 84%, а за 2020 год — 88%.

Проведённые эксперименты нашли своё отражение в законодательстве. Для возможности использования дистанционной идентификации с помощью ПВДНП в целях создания и выдачи квалифицированных сертификатов указанный вид идентификации был внесён регуляторами по предложению Сбербанка в закон № 63-ФЗ «Об электронной подписи» (в редакции закона от 27 декабря 2019 г. № 476-ФЗ).

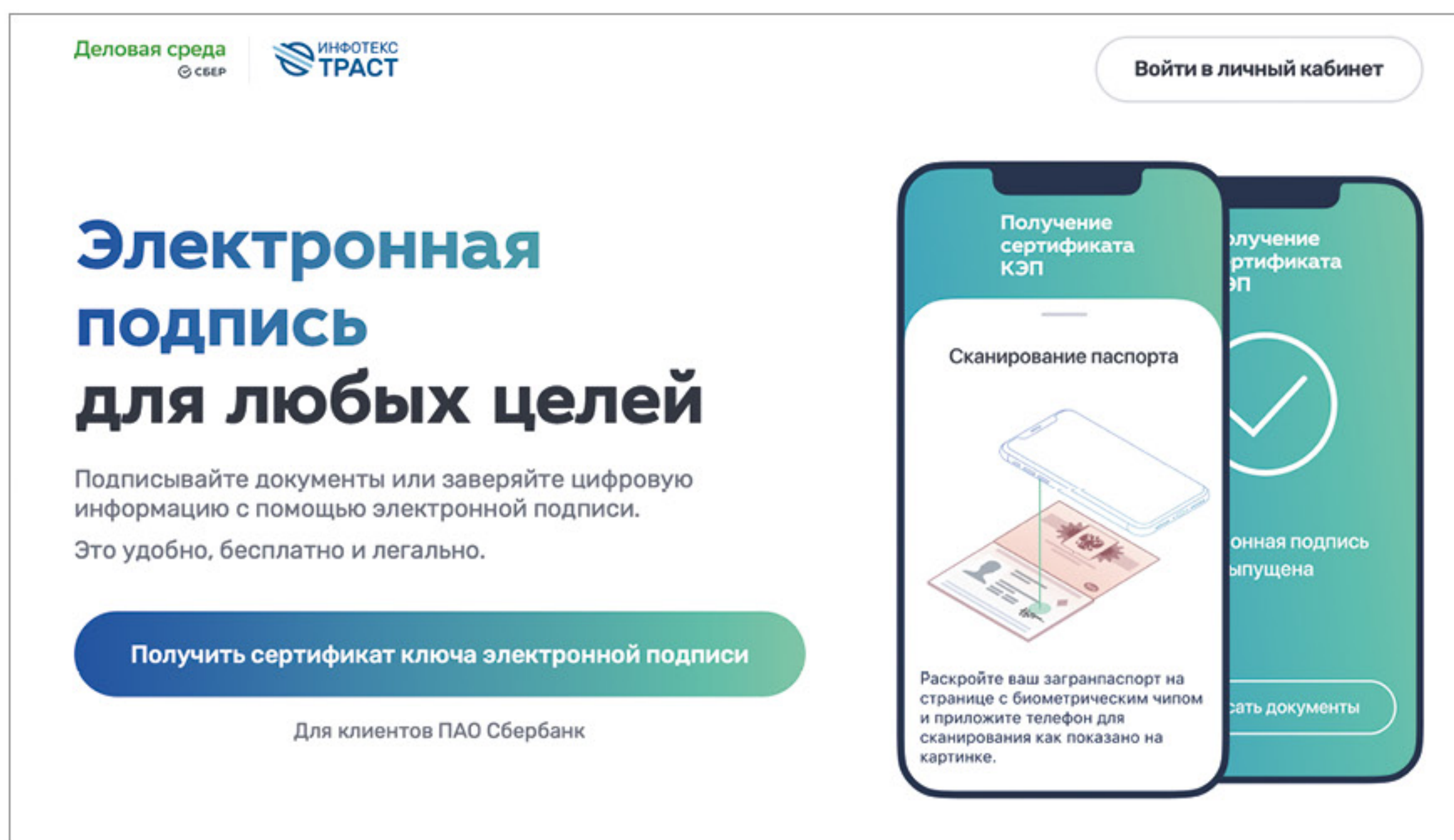


Рисунок 5. Сервис dsign.dasreda.ru

Кроме того, в 2020 году дочерняя компания Сбербанка АО «Деловая среда» и ОАО «Инфотекс Интернет Траст» запустили на базе технологии мобильной подписи бесплатный сервис, с помощью которого физические лица могут создавать, использовать и хранить квалифицированные ЭП в онлайн-режиме (<https://dsign.dasreda.ru/>). Весь процесс проходит онлайн в несколько шагов и занимает не более десяти минут, при этом установление личности получателя ЭП производится дистанционно, с помощью биометрического загранпаспорта и мобильного приложения, поддерживающего NFC-технологию.

ЗАКЛЮЧЕНИЕ

На наш взгляд, разработанные инновационные технологии мобильной усиленной квалифицированной ЭП и дистанционной криптографической идентификации, а также созданный на их основе сервис РБиДОС позволили полностью реализовать цели проведенных экспериментов.

Сбербанком был создан важный для Российской Федерации сервис регистрации бизнеса и открытия счетов, функционирующий в режиме 24×7×365, с высоким уровнем обслуживания и технической поддержки. Сервис РБиДОС позволил реализовать возможность беспшовного старта бизнеса за счёт внедрения процедуры открытия расчётного счёта полностью дистанционно либо всего за один визит в отделение банка или офис партнёрской сети. Также сервис позволил продолжить регистрацию бизнеса в России во время пандемии,

снизил риски для здоровья предпринимателей за счёт минимизации социальных контактов.

Сервис РБиДОС значительно улучшил клиентский путь, так как позволил провести не только регистрацию бизнеса, но и открытие счёта в Сбербанке не выходя из дома либо всего за один визит в офис банка или его партнёров.

В целях развития цифровизации экономики Российской Федерации целесообразно продолжить внедрение и дальнейшее развитие указанных технологий как в рамках созданного сервиса, так и в других сферах. Предлагаем предусмотреть следующие мероприятия:

- ♦ создать на базе сервиса РБиДОС общедоступный суперсервис (например, на портале Госуслуг) и реализовать возможность подключения к нему широкого круга кредитных организаций;

- ♦ обеспечить возможность проходить дистанционную биометрическую идентификацию с использованием государственных систем ЕСИА и ЕБС для получения квалифицированных сертификатов;

- ♦ реализовать на базе платформы СЗАС типовое решение, позволяющее проводить её интеграцию с клиентскими мобильными приложениями, средствами удостоверяющих центров, системами дистанционного банковского обслуживания и электронного документооборота;

- ♦ интегрировать типовое решение на базе СЗАС с государственными удостоверяющими центрами, уполномоченными на выпуск сертификатов ЮЛ и ИП, а также обеспечить возможность использования предпринимателями мобильной ЭП на базе такого типового решения.



Александр
БОДРИК
эксперт BIS Journal

БЕЗОПАСНОСТЬ PROD-УРОВНЯ

МАСШТАБНАЯ, НО ЗАХВАТЫВАЮЩАЯ ВООБРАЖЕНИЕ ЗАДАЧА

Цифровая трансформация делает классические неИТ-компании провайдерами цифровых услуг для правительства, клиентов и сотрудников. Это значит, что компаниям придётся внедрить практики управления приложениями, что позволит оказывать таковые услуги с заданным уровнем сервиса — будь то классическая доступность, время генерации счёта, время формирования квоты или любой другой важный для цифрового потребителя параметр.

Одной из фундаментальных практик управления приложениями является разделение ИТ-ландшафта на среды. Выросшие из классических инфраструктурных задач подразделения информационной безопасности обычно знают три таких среды — PROD/TEST/DEV. Однако для по-настоящему крупных цифровых сервисов с миллионами клиентов онлайн три среды недостаточно, и необходимо внедрять дополнительные.

ДОПОЛНИТЕЛЬНЫЕ СРЕДЫ ДЛЯ УПРАВЛЕНИЯ ПРИЛОЖЕНИЯМИ

Mirror-среда. Дублирует PROD, как и PROD, содержит клиентские данные, позволяет воссоздать инцидент недоступности сервиса или его компонента контролируемым образом. Требует применений тех же контролей безопасности и с такой же частотой, что и PROD.

Pre-prod-среда. Максимально близка к PROD, но не содержит клиентских данных. Между pre-prod и PROD разумно организовать ворота безопасности (security gate), например, сканируя конфигурации и образы Docker на наличие уязвимостей и соответствие требованиям безопасности. Тут же оптимально проводить тесты на проникновение и сканирование на уязвимости.

Obfuscation-среда. Позволяет провести обфускацию клиентских данных для передачи обфусцированных данных вне контура с клиентскими данными.

DR-среды. Дублируют PROD и готовы подхватить задачи PROD в случае значительных проблем.

МЕХАНИЗМЫ СИНХРОНИЗАЦИИ КИБЕРБЕЗОПАСНОСТИ С УПРАВЛЕНИЕМ ПРИЛОЖЕНИЯМИ

Change Advisory Board. Комитет по согласованию изменений, рекомендуется ITIL, в случае наличия изменений, драйвером которых выступает служба ИБ, приглашает представителя службы ИБ. В случае отказа в согласовании такого изменения служба ИБ запускает процесс риск-менеджмента, дабы документировать отказ и бизнес-причины для него и проверить наличие спонсора принятия риска, например представителя высшего руководства.

Promotion. Постепенное тестирование всех вносимых изменений на каждой из сред, пока изменение не будет внесено в PROD.

Production Schedule. Расписание внесений изменений в PROD. Важно планировать окна обслуживания для применения фиксов безопасности наперёд.

Verification. Проверка исполнения изменения, например, фикса log4j путём сканирования Qualys/Nessus.

Passive/Active Security Gates. Пассивный (мониторинговый) режим работы ворот безопасности и активный. В пассивном режиме повышение фикса не блокируется в случае наличия критических проблем с безопасностью. А в активном режиме — блокируется.

Proactive Security. Подход проверки безопасности, например, безопасности кода (SAST, SCA) на ранних средах, с изменением режима работы ворот безопасности по мере приближения к PROD.

Security Patching timelines. Формальные обязательства службы управления приложения перед службой ИБ по применению фиксов в случае наличия уязвимостей различного уровня. Например, High/Critical CVSS — 14 календарных дней.

Ticket. Заявка в используемой службой поддержки системе HelpDesk позволяет отслеживать количество запросов ИБ и одновременно оперативность их обработки службой управления приложениями.



Security Officer. Отвечающий за безопасность крупного приложения (ERP, BSS, core banking system) специалист координирует работу различных служб по обеспечению безопасности. Может быть специалистом по ИБ, в случае отсутствия такового эта функция так или иначе оказывается на директоре по управлению приложениями.

ТИПОВЫЕ МЕРЫ БЕЗОПАСНОСТИ ДЛЯ КРУПНЫХ ПРИЛОЖЕНИЙ

Мониторинг безопасности. Применение известных HIDS/EDR, SIEM и Vulnerability Scanning, Penetration Testing для мониторинга состояния безопасности крупных приложений.

Application Security. Применение классических SAST, SCA и обучения разработчиков, постепенное включение крупных приложений в процессы Application Security.

Container Security. Набор практик по обеспечению безопасности контейнеризованных приложений, в том числе управляемых с помощью Kubernetes/OpenShift. Традиционно включает сканирование образов контейнеров, мониторинг активности контейнеров (runtime

security), харденинг кластеров Kubernetes/OpenShift, управление привилегиями ролей внутри кластеров Kubernetes/OpenShift, сканирование конфигурации Kubernetes/OpenShift на предмет проблем безопасности (IaaS Security).

Cloud Security. Набор практик по обеспечению безопасности используемых облачных провайдеров (AWS/Azure/GCP/Alibaba). Включает в себя мониторинг безопасности облака (встроенные Defender/GuardDuty/Security Hub, отдельные средства CSPM), управление секретами / API ключами (Secrets Management — Vaults, Hashicorp Vault), IaaS Security, Cloud IAM.

ЗАКЛЮЧЕНИЕ

Обеспечение безопасности крупного приложения — масштабная, но захватывающая воображение задача. Возможно, главное — беспощадная приоритизация подзадач и построение продуктивных рабочих взаимоотношений со службами потребителями безопасности (бизнес, юристы) и службами поставщиками тех или иных сервисов безопасности — AppSec, SOC, DevOps, administrators.

ПОЧЕМУ БАНКИ НЕ ВИТАЮТ В ОБЛАКАХ?

КАКИЕ БАРЬЕРЫ СТОЯТ НА ПУТИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ И КАК ИХ ПРЕОДОЛЕТЬ



Иван ГУЗЕВ
руководитель
направления
Облачные сервисы
Ассоциации ФинТех

Облачные сервисы позволяют бизнесу применять готовые IT-решения вместо создания собственной дорогостоящей инфраструктуры. Российские компании активно мигрируют в «облака». Финансовый сектор также заинтересован во внедрении облачных технологий, но существуют препятствия, затрудняющие этот процесс. Какие барьеры стоят на пути финансовых организаций и как их преодолеть?

Облачные сервисы и технологии во всём мире развиваются стремительными темпами, практически по экспоненциальной кривой. Согласно прогнозам исследовательской компании Statista, в 2022 году объём мирового рынка публичных облачных сервисов вырастет примерно на 22 % и составит порядка \$ 482 млрд.

Финансовые организации активно пользуются облачными решениями. Так, согласно данным Cloud Security Alliance, в мире порядка 91 % банков используют публичные облачные сервисы или планируют это сделать в ближайшие шесть-девять месяцев. Кроме того, на данный момент многие финансовые организации (73 %) переносят большое количество критичных бизнес-процессов в облака, и этот процент растёт с каждым годом.

Российские финансовые организации также внедряют облачную инфраструктуру, но в настоящее время не могут в полной мере использовать предлагаемые разработчиками решения.

БАРЬЕРЫ И ПРОБЛЕМЫ

Ассоциация ФинТех провела опрос крупнейших компаний финансовых рынков, чтобы определить, какие вызовы с точки зрения развития облачных технологий являются наиболее критичными.

В ходе опросов выяснилось, что представители финансового рынка обеспокоены обеспечением безопасности данных при использовании облачных сервисов, сложностью миграции в «облака», неготовностью приложений к работе в таком формате и нехваткой компетенций. Кроме этого, участники рынка называют в числе возможных проблем увеличение шанса потери или утечки данных, сложности контроля самого облачного провайдера, а также отсутствие регулирования в этой сфере.

Можно назвать пять основных барьеров использования публичных облачных сервисов финансовыми организациями в России:

1. Запрет передачи банковской тайны третьим лицам, а также передачи персональных данных (ПДн) третьим лицам без согласия субъекта ПДн;
2. Отсутствие стандартов и регуляторных требований по обеспечению информационной безопасности для провайдеров облачных услуг;
3. Отсутствие нормативной базы по оценке надёжности провайдеров облачных сервисов;
4. Отсутствие доверенной среды аудиторов по контролю за облачными провайдерами;
5. Отсутствие требований и механизмов по разграничению зон ответственности при предоставлении облачных сервисов.

Эти барьеры связаны со следующими проблемами:

1. Проблема с передачей чувствительных данных для финансовых организаций, таких как банковская тайна и персональные данные. В случае с персональными данными ситуация понятна, хоть и сложна с точки зрения передачи на аутсорсинг. В вопросе передачи банковской тайны в «облако» пока существует недопонимание со стороны финансового рынка.

2. Проблема с точки зрения регулирования. В России существуют большое количество требований по информационной безопасности, но они не направлены на работу с облачными сервисами, и в каждом отдельном случае компании необходимо самой «накладывать» их на сервисы, предоставляемые облачными провайдерами.

Также отсутствуют требования к самим провайдерам облачных услуг.

3. Проблема разграничения зоны ответственности. На данный момент независимо от того, обрабатывает данные облачный провайдер или обработка идёт вне зависимости от типа предоставляемого сервиса, ответственность за этот процесс несёт финансовая организация.

МЕЖДУНАРОДНЫЙ ОПЫТ

С точки зрения вопроса передачи чувствительных данных, ситуация неоднозначная. Например, в Сингапуре разрешено передавать данные без глобальных ограничений, но только



Рисунок 1. Основные проблемы и направления их решения

для реализации аутсорсинга бизнес-процессов. В Европейском Союзе передача данных разрешается, но исключительно с согласия держателей данных. В США разрешается передача таких данных, но с уведомлением клиентов о раскрытии данных, от которого субъект данных вправе отказаться. В швейцарской практике раскрытие данных может происходить лишь в случае, когда сотрудники поставщика облачных сервисов оформлены в качестве представителей банка. Несмотря на ряд различий, во всех вышеупомянутых примерах абсолютно точно и ясно определено, разрешена передача данных или нет, какие данные можно передавать и в каких ситуациях возможна их передача.

Что касается регулирования, то здесь, напротив, можно выделить единый подход. В США, ЕС, Сингапуре и Японии регулирование направлено на стандартизацию облачных сервисов и облачных провайдеров. Существуют отдельные организации, занимающиеся стандартами, их доработкой и внедрением, обсуждением стандартов с участниками рынка. Например, мировым лидером по определению передовых методов обеспечения безопасной среды облачных вычислений выступает международная организация Cloud Security Alliance, взаимодействующая с отраслевыми экспертами, ассоциациями, правительствами и корпорациями по вопросам облачной безопасности. Также подобные организации следят за новыми тенденциями в области облачных технологий и создают основу для доверенного аудита по этим стандартам.

Что касается вопроса разделения ответственности, единого стандарта в международной практике нет. Если речь идет о персональных данных, то в европейских странах, с учетом появления Общего регламента по защите данных (GDPR), появилось разделение ответственности на законодательном уровне, где есть оператор и обработчик персональных данных и у каждого участника определена зона ответственности. Такая же система распределения ответственности присутствует в Стандарте безопасности данных индустрии платёжных карт (PCI DSS) в разделе

обработки данных. Что касается других категорий данных, чёткого распределения ответственности на данный момент не разработано, однако в странах ЕС и в целом в мире существует определённый налаженный механизм и апробированное страхование ответственности облачного провайдера перед финансовыми организациями, что позволяет преодолеть данный барьер.

КАК ПРЕОДОЛЕТЬ БАРЬЕРЫ?

Для того чтобы российские финансовые организации могли преодолеть вышеперечисленные барьеры, на мой взгляд, необходимо предпринять следующие шаги:

- 1) определить в нормативно-правовых актах, какие данные и при каких условиях можно передавать на аутсорсинг провайдерам облачных услуг;
- 2) определить требования к облачным провайдерам для того, чтобы финансовым организациям было легче прогнозировать операционный риск и риск информационной безопасности при переходе к облачным провайдерам;
- 3) создать доверенную среду аудита облачных провайдеров;
- 4) определить механизмы разграничения ответственности между финансовыми организациями и провайдерами в случае использования облачных сервисов.

Использование облачных сервисов оказывает положительный эффект на деятельность компаний. Это даёт возможность оптимизировать бизнес-процессы, сократить операционные издержки и, соответственно, получить конкурентные преимущества.

Учитывая вышесказанное, развитие рынка публичных облачных сервисов в России обладает существенным потенциалом. Устранение барьеров для использования облачных сервисов имеет приоритетную важность и требует слаженного взаимодействия регуляторов и участников рынка.

Среди ключевых вызовов в использовании облачных технологий участники рынка выделяют:

- риск потери или утечки данных при использовании публичных облачных сервисов или услуг высокотехнологичного аутсорсинга;
- регуляторные риски в связи с отсутствием четких требований информационной безопасности в отношении внешних сервисов и закрепленной ответственности поставщиков таких решений за нарушение SLA и утечку данных;
- расходы на контроль и оценку рисков информационной безопасности при использовании публичных облачных сервисов или услуг hi-tech аутсорсинга;
- регуляторные ограничения при хранении и обработке персональных данных, банковской тайны в инфраструктуре поставщика публичных облачных сервисов и неоднозначность толкования отраслевых требований к данным.

Рисунок 2. Ключевые вызовы в использовании облачных технологий по мнению участников рынка



Константин ГРАЧЁВ
руководитель
службы
информационной
безопасности
КБ «Максима» (ООО)



Оксана ДОКУЧАЕВА
главный специалист
отдела мониторинга
и оценки рисков
сетевой безопасности
Дирекции
информационно-
технологических
систем и систем связи
ГУП «Московский
метрополитен»



**Анастасия
НИКОЛАЕВА**
начальник
службы ИБ
КБ «АРЕСБАНК»

ПРИВЕСТИ В СООТВЕТСТВИЕ!

О РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ГОСТ 57580 В НЕКРЕДИТНЫХ ОРГАНИЗАЦИЯХ

В 2019 году Банк России выпустил Положение № 684-П, устанавливающее обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков. Указанное Положение, в частности, основывается на требованиях пункта 6.9 ГОСТ Р 57580.2–2018 и в этой части вступает в силу с 1 января 2022 года.

Таким образом, к январю 2022 года некредитные финансовые организации должны привести в соответствие с этим Положением и требованиями ГОСТ свои процессы и организационно-распорядительные документы.

Проблемой для некредитных финансовых организаций может стать необходимость выполнения требований пп. «г» и «д» п. 6.9 ГОСТ:

г) *третий уровень соответствия: организационные и технические меры процесса системы ЗИ реализуются в значительном количестве на постоянной основе в соответствии с общими подходами (способами), установленными в финансовой организации. Контроль и совершенствование реализации организационных и технических мер процесса системы ЗИ осуществляются бессистемно и/или эпизодически;*

д) *четвёртый уровень соответствия: организационные и технические меры процесса системы ЗИ реализуются в полном объёме на постоянной основе в соответствии с общими подходами (способами), установленными в финансовой организации. В финансовой организации в основном реализованы контроль и совершенствование реализации организационных и технических мер процесса системы ЗИ.*

Указанные требования аналогичны требованиям, предъявляемым к банкам, однако некредитные финансовые организации в большинстве случаев значительно меньше банков, и выполнение данных требований может вызвать ряд проблем.

Так, из наиболее распространённых сложностей можно выделить недостаток квалифицированных специалистов в области информационной безопасности, недостаточное

финансирование и невозможность заложить в бюджет средства на закупку требуемого оборудования и средств защиты информации, кроме того, сами средства защиты информации в большей степени рассчитаны на крупные организации, а не на небольшие компании, и не тестировались на таких площадках.

Таким образом, исполнить требования 684-п в срок могут себе позволить только крупные игроки, в той или иной степени уже их соблюдающие.

Между тем проверки со стороны регуляторов небольших организаций могут привести к масштабному применению штрафных санкций и дестабилизации рынка НКФО.

В качестве решения данной проблемы разумно применить следующий подход:

- ◆ провести аудит системы защиты информации в организации;
- ◆ определить, какие организационные меры могут быть применены наиболее безболезненно и срочно;
- ◆ привлечь внешних специалистов для разработки необходимых организационно-распорядительных документов;
- ◆ переобучить штатных специалистов по информационной безопасности.

Разумеется, быстрее и эффективнее с точки зрения приближающейся проверки ЦБ РФ исполнить требования, связанные с разработкой организационно-распорядительных документов, так как это проще и дешевле, чем закупить оборудование и СЗИ и подобрать необходимых специалистов.

Представляется целесообразным разработать или актуализировать следующие документы (перечень примерный):

- ◆ политика по информационной безопасности;
- ◆ положение о службе/отделе/сотруднике по информационной безопасности;
- ◆ положение по оценке рисков нарушения информационной безопасности;
- ◆ порядок действий сотрудников в случае возникновения инцидентов, связанных с ИБ;
- ◆ отчёты о результатах служебного расследования инцидента ИБ;



- ◆ положение о модели угроз и нарушителей информационной безопасности;
- ◆ инструкция пользователя по обеспечению информационной безопасности на рабочей станции;
- ◆ регламент настройки средств защиты от воздействия вредоносного кода;
- ◆ регламент настройки SIEM-системы (при наличии);
- ◆ регламент настройки системы обнаружения вторжений (при наличии);
- ◆ регламент настройки системы предотвращения утечек информации (при наличии);
- ◆ регламент настройки сканера уязвимостей (при наличии);
- ◆ регламент настройки технических мер системы защиты информации;
- ◆ политика обработки персональных данных;
- ◆ план действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения нестандартных и чрезвычайных ситуаций;
- ◆ регламент по управлению инцидентами информационной безопасности;
- ◆ порядок, регламентирующий процесс повышения знаний; обучение сотрудников в рамках требований по ИБ;
- ◆ план проведения обучения сотрудников по ИБ;
- ◆ ведомость планового, повторного инструктажа сотрудников;
- ◆ отчёты по проведению внешнего аудита по выполнению требований положений Банка России;

- ◆ внутренние отчёты проверок;
- ◆ план мероприятий по информационной безопасности;
- ◆ отчёт по проведённым контрольным мероприятиям по ИБ;
- ◆ утверждённый перечень объектов информационной инфраструктуры;
- ◆ утверждённый перечень технологических участков с кодами регистрации событий и регламентация процесса.

Отдельное внимание следует уделить вопросу профессионального образования и повышению квалификации. В настоящее время ситуация такова, что специалистов по информационной безопасности, работающих с некредитными финансовыми организациями, довольно мало, чаще всего специалисты не знают специфику НКФО.

* * *

При этом на различных форумах и конференциях, где специалисты могут обменяться опытом, секции по безопасности в НКФО практически отсутствуют, что является упущением со стороны организаторов таких мероприятий.

Разумно предположить, что повышение внимания к проблемам НКФО является необходимым и, несмотря на возникающие в связи с возросшими требованиями регуляторов проблемы, может дать толчок к развитию нового актуального направления в сфере информационной безопасности.



МЫ С ТОБОЙ ДВА БЕРЕГА У ОДНОЙ РЕКИ...

ЭССЕ О ТОМ, О ЧЁМ НЕ ДУМАЮТ, КОГДА ДУМАЮТ
О БЕЗОПАСНОСТИ ИНФОРМАЦИИ



Сергей ВИХОРЕВ
советник
генерального
директора
ООО «ИТ-Экспертиза»

Скажу сразу, статью «Привести в соответствие! О реализации требований ГОСТ 57580 в некредитных организациях» прочитал несколько раз. После первого — АХ! После второго — ОХ! А после третьего — а почему бы и не может быть? В общем, статья натолкнула меня на мысли, может быть, и не связанные с её содержанием (хотя почему бы и нет)? Но об этом чуть позже. А сейчас о сути.

ЧТО БЫЛО, ЧТО БУДЕТ, ЧЕМ СЕРДЦЕ УСПОКОИТСЯ

Начнём, пожалуй, с того, что Положение № 684-п уже не действует. Его заменило Положение № 757-п, которое действует с лета 2021 года. Будем аккуратно относиться к нормативным документам. Конечно, разница невелика, но всё-таки она есть. Во-первых, включены организации, работающие с криптовалютами (цифровые финансовые активы). Во-вторых, существенно (и это

очень важно!) изменён перечень некредитных финансовых организаций, выполняющих требования ГОСТ 57580. Главное здесь то, что определён перечень организаций, соответствующих минимальному уровню защиты информации.

Отметим, что для организаций, соответствующих минимальному уровню защиты, ни сроки, ни требования по соответствию систем защиты информации не определены. Это уже намного легче. Ну и, конечно, важно, что для организаций, реализующих только усиленный и стандартный уровни защиты информации, обеспечение четвёртого уровня соответствия, предусмотренного подпунктом «д» пункта 6.9 ГОСТ Р 57580.2–2018, отложено аж до 01.07.2023.

Что из этого следует? Во-первых, круг организаций, которым необходимо обеспечить усиленный и даже стандартный уровень защиты информации, не такой уж и большой. И это, как правильно отмечено в статье, «крупные игроки». Во-вторых, время ещё есть, и привести в



соответствие свои системы защиты информации вполне возможно.

Теперь о бюджетах. Помнится, когда появились требования к защите персональных данных, некоторые эксперты (не будем показывать пальцем) прогнозировали затраты на их защиту в размере ВВП страны. Однако время прошло, защита персональных данных есть, а затраты в размере ВВП — не оправдались. Почему? Потому что при анализе были допущены системные ошибки. С одной стороны, не учитывалось, что часть функций безопасности уже реализуется в интересах ИТ-служб (но об этом чуть ниже). С другой — компьютерная техника устаревает, и это происходит, дай бог, каждые 3–5 лет. И такие деньги на модернизацию закладываются. Вот и защиту информации возможно сделать в счёт этого бюджета. Получается, не так страшен чёрт, как его малюют.

Последнее. В статье приведён достаточно мощный перечень документов. Правильный ли он? Наверное, да. Нужен ли он? Наверное, нет. Не надо переключаться на старорежимный бюрократический язык. Я, как старый бюрократ, понимаю, что чем больше бумаги, тем спокойнее. Но бумага не может защитить информацию, она только создаёт определённый иммунитет, позволяющий привлечь к ответственности злоумышленника. Я думаю, здесь важнее вопросы, которые должны быть зафиксированы (а они в статье изложены правильно!), а вот в каком документе

и как — это дело руководителя объекта, тем более что официального перечня документов нет. Да, понимаю, что приходят проверяющие и требуют, чтобы было так и никак иначе. Но это совсем другая проблема: проблема подготовки квалифицированных проверяющих кадров. Вот и получается, что прежде всего готовить нам надо кадры экспертов, а остальное — дело времени.

А ДАВАЙТЕ ТЕПЕРЬ ПОДУМАЕМ...

Все мы учили в школе, что две параллельные прямые не пересекаются. Однако это утверждение было справедливо только для евклидовой геометрии. Оказалось, стоит взглянуть на проблему с другой стороны, как оно оказывается ложным. Аксиоматика планиметрии Лобачевского отличается от аксиоматики планиметрии Евклида, и уже две параллельные прямые могут пересечься в одной точке. Так, может, и в нашей проблеме обеспечения безопасности информации это приемлемо?

Давайте не будем рассуждать об этой важной проблеме только с точки зрения безопасника. AD — это чья система? ИТ или ИБ? Думаю, что ни один сисадмин не представляет свою жизнь без этой компоненты. А если в СУБД не разделить полномочия пользователей, насколько снизится производительность? И чья это проблема: безопасности или всё-таки ИТ-структур? Вот и получится, что разделить нельзя...

Несколько лет назад я на своём дачном участке посадил берёзу. А она дала от одного корня два ствола, вернее, сначала был один, а потом — два. И оба равные! И растут они порознь, но ветками тянутся друг к другу. И уж не знаю, кто из них главнее. Так и в соотношениях ИТ и ИБ: кто главнее? Да никто! Все мы от одного корня — информации. Только задачи у нас разные, но корень — один! И что, будем бодаться или будем брататься? На мой взгляд, правильнее второе. И исходя из этого получается следующее.

1. Давайте примем за аксиому, что решить проблему ИБ-безопасности, как и проблему ИТ-обеспечения процесса обработки информации, без совместных усилий невозможно.

2. Тезис «Кадры решают все» актуален и в наши дни. Поэтому надо прежде всего уделить внимание исключению инсайдерских действий.

3. Только совместное действие ИБ- и ИТ-инфраструктур может привести к положительному результату.

4. Надо понимать: то, что хорошо для ИБ, приемлемо и для ИТ.

Это потребует серьёзного диалога между ИТ и ИБ, о чём мы раньше не задумывались. Не могу сказать, что ожидаемый диалог будет спокойным и безоблачным, но его надо начинать.

ДАВАЙТЕ НЕ БУДЕМ ДЕЛИТЬ ПОЛЯНУ

В ОДНОЙ ИЗ СОСЕДНИХ СТРАН НЕТ СПЕЦИАЛИСТОВ-ИБЭШНИКОВ, ТАМ ЗА ИНЦИДЕНТЫ ИБ НАКАЗЫВАЮТ РУКОВОДИТЕЛЕЙ ИТ



**Василий
ОКУЛЕСКИЙ**
эксперт, кандидат
технических наук

Традиционно новые темы начинаются с «прожарки», и Сергей Викторович Вихорев это сделал, как всегда, блестяще. Должен согласиться с ним и обратить внимание авторов статьи «Привести в соответствие! О реализации требований ГОСТ 57580 в некредитных организациях», что нынче действительно актуально положение Банка России № 747-П от 2021 года. И это, с одной стороны, серьёзно сужает круг организаций, должных реализовывать стандартный и усиленный уровень защиты, а с другой — формирует требования к новациям финансового рынка — акторам цифровых активов, что само по себе составляет маленькую революцию.

Эти замечания не делают статью неактуальной, наоборот, мне, как практику, статья понравилась поднятием как минимум двух тем:

1. Рассматриваемые категории субъектов нормотворчества БР никто ранее не регулировал, поэтому для них мало что адаптировано, и про них очень мало говорили на профессиональных банковских площадках, особенно касаясь цифровых активов.

2. В статье поднята тема организационных мер как начального подхода к обеспечению ИБ и дан довольно полный перечень документов «с чего начать». Сам по себе этот посыл — уже плюс.

Не буду дискутировать о наборе документов и глубине их проработки, технической поддержке решений «по ИБ», уверен, что значительное число задач по ИБ уже решается подразделениями ИТ и им не хватает лишь (?) методической

поддержки с точки зрения ИБ, а это уже вопрос зрелости компании.

Чтобы ответить на вопрос о достаточности набора документов, могу предложить простое упражнение: надо составить табличку направлений защиты (совокупность выбранных для организации организационных и технических мер в соответствии с выбранным уровнем защиты) и имеющимися внутренними нормативными документами (ВНД), пустые клетки в этой табличке будут говорить об отсутствии необходимого ВНД. Для полноты картины можно указать там же те документы четвёртого уровня, которые будут подтверждать выполнение этого требования. Полезный инструмент для офицера безопасности и для аудитора.

В предложенном перечне документов было бы правильно акцентировать внимание на контроле жизненного цикла прикладного программного обеспечения, работающего с использованием сети Интернет, особенно при наличии собственной разработки.

Чего не хватает в статье, так это более широкого взгляда на проблему соответствия требованиям.

В очередной раз в нормативных документах БР требования к аудиторам сводятся лишь к наличию лицензии ФСТЭК у организации, осуществляющей проверку. А ведь при требованиях внешней проверки должны быть определены специальные профессиональные требования к аудиторам по принципам типа аудиторов PCI DSS, с обязательным периодическим подтверждением соответствия этим требованиям. Определена юридическая и финансовая ответственность компаний-аудиторов, порядок аккредитации таких компаний, разработаны и утверждены (кем?) программы обучения и аттестации аудиторов. Если не будут решены эти проблемы, говорить о каком-то существенном прорыве в обеспечении информационной безопасности просто несерьёзно.

И в заключение ещё раз подчёркиваю: статья нужная и направление её правильное.

Могу предложить простое упражнение: надо составить табличку направлений защиты и имеющихся внутренних нормативных документов (ВНД). Пустые клетки в этой табличке будут говорить об отсутствии необходимого ВНД

МОБИЛЬНАЯ ПОДПИСЬ — МАКСИМАЛЬНОЕ УДОБСТВО И БЕЗОПАСНОСТЬ

Мобильная подпись — это технология, использующая мобильное приложение для хранения ключа подписи на мобильном устройстве пользователя. Хранение ключа подписи в мобильном приложении, а не на персональных носителях (USB-токены, смарт-карты и пр.) и не на сервере является главным отличием мобильной подписи от классической и дистанционной («облачной») подписи соответственно.

ВЫСОКАЯ СТЕПЕНЬ ЗАЩИТЫ КЛЮЧЕЙ ОТ КОМПРОМЕТАЦИИ

Ключи пользователей безопасно создаются и хранятся в приложении мобильного телефона пользователя, всегда находящегося под рукой, доступ к которому может быть защищен индивидуальными паролями, а также современными технологиями Touch ID или Face ID.

ПОДЛИННАЯ МОБИЛЬНОСТЬ ПОДПИСИ

Забудьте про связку из токенов, USB-хаб и установку драйверов. Вы больше не будете привязаны к одному рабочему месту и сможете формировать документы в любом окружении, например, на ПК, в СЭД или в самом мобильном устройстве, и подписывая их со своего смартфона.

КВАЛИФИЦИРОВАННАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ

Мобильные приложения **КриптоПро** DSS Client и myDSS 2.0, содержащие ключ подписи, позволяют подписывать документы непосредственно на мобильном устройстве в том числе квалифицированной электронной подписью, поскольку в своем составе используют сертифицированное средство **КриптоПро** CSP 5.0 R2.

СОХРАНЕНИЕ ИНВЕСТИЦИЙ

Вам не придется менять или сильно дорабатывать систему документооборота. Не нужно отказываться от привычного ПО для работы с электронной подписью. Все, что умеет работать со стандартом де-факто российского рынка средств ЭП — **КриптоПро** CSP, при установке мобильного приложения бесшовно сможет использовать мобильную подпись.

СНИЖЕНИЕ СТОИМОСТИ ВЛАДЕНИЯ

На рабочее место пользователя установка средств электронной подписи не требуется. Достаточно установить легковесное и простое в использовании мобильное приложение на его смартфон. Работу по настройке всех криптографических механизмов и форматов возьмут на себя серверные компоненты (**КриптоПро** DSS). Отсутствие средств электронной подписи на рабочем месте пользователя позволяет существенно сократить расходы на их приобретение, настройку, сопровождение и обновление.

КриптоПро

@ info@cryptopro.ru

+7 (495) 995-48-20

@CryptoProInfoBot

<https://cryptopro.ru>



Александр ШМЕЛЕВ
руководитель направления
консалтинга по информационной
безопасности, AKTIV CONSULTING

МАСШТАБ КИБЕРАТАК

ВЫВОДИТ ИБ В БАНКАХ НА НОВЫЙ УРОВЕНЬ

Сразу несколько видов кибератак на частных пользователей и инфраструктуру финансовых организаций вышли в 2021 году на очередной виток развития. Стоит ожидать, что в 2022 году эти технологии сделают ещё больший скачок вперёд. Примечательно, что данные проблемы постепенно затрагивают всё больше подразделений финансовых организаций и перестают быть проблемами исключительно специалистов по ИБ. Для их решения банкам рано или поздно придётся пойти на усиление киберзащиты, внедрение многоканального антифрода и многофакторной аутентификации. При этом, защищаясь только лишь от избранных угроз, значительные потери можно понести именно там, где угроза казалась несущественной. Поэтому защита сегодня должна быть комплексной, предполагающей предотвращение угроз, а не работу с инцидентами. Отталкиваться от постулата «убытков нет, значит, защита не нужна» сегодня очень опасно.

РОСТ РОЛИ ИБ В БИЗНЕС-СТРАТЕГИИ ФИНАНСОВОЙ ОРГАНИЗАЦИИ

Говоря о противостоянии киберугрозам, нельзя не сказать о недавних

изменениях в регуляторике, предписывающей соблюдение требований для обеспечения кибербезопасности в финансовой сфере. В 2021 году появился целый ряд новых Положений Банка России, в часть ранее существовавших внесены изменения. Но одним из наиболее значимых для обеспечения информационной безопасности в финансовых организациях нормативных актов стало Положение Банка России 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе». Основным смыслом этого Положения заключается в отнесении киберрисков к разряду операционных и необходимости резервирования под них определённых денежных средств. Большая часть требований документа вступает в силу в январе 2022-го. Однако многие участники рынка до сих пор не провели полноценную работу для их реализации. Проблема заключается в том, что сотрудникам, отвечающим за операционные риски в организации, необходимо разработать методику оценки рисков, создать математические и вероятностные модели их расчёта. Зачастую в финансовых организациях нет выделенных риск-офисов, и вопрос выполнения

требований Положения 716-П перекладывается на плечи специалистов по информационной безопасности, не обладающих компетенциями по оценке операционных рисков. И это, конечно, серьёзная проблема, которую сообществу профессионалов ИБ предстоит решать вместе. В то же время есть и другая сторона медали: 716-П обязывает резервировать средства и под киберриски, тем самым смещая фокус внимания бизнеса в сторону информационной безопасности. Это тот самый момент, когда регуляторика может помочь функции ИБ интегрировать себя в достижение бизнес-показателей организации, а значит, начать вести конструктивный диалог с руководством на одном языке. Таким образом, можно констатировать, что Положение 716-П — это новый виток развития не только в вопросах регулирования информационной безопасности в финансовых организациях, но и вообще начало смены парадигмы, где ИБ существует особняком.

ВРАГ У ВОРОТ — УКРЕПЛЯЕМ АНТИФРОД

В 2021 году в финансовых организациях, как и во многих других отраслях, серьёзно укрепился тренд удалённой работы. В условиях пандемии многие кредитные организации сочли целесообразным организовать работу большинства сотрудников вне офиса. И открыли тем самым массу возможностей для злоумышленников. По различным оценкам ущерб от вирусов-вымогателей по итогам 2021 года в целом по рынку составляет 20 млрд долларов.

Защищаясь только лишь от избранных угроз, значительные потери можно понести именно там, где угроза казалась несущественной. Поэтому защита сегодня должна быть комплексной

Атаки подобного рода были таргетированными и хорошо подготовленными. Их причиной стала заниженная оценка рисков ИБ и, как следствие, недостаточные меры защиты финансовых организаций. Интересно, что сейчас появились решения, в той или иной мере защищающие от подобной проблемы: сервисы, которые не позволяют вирусу-шифровальщику шифровать данные. Они не избавляют от самого заражения, но способны хотя бы уберечь организации от потери данных.

Ещё одной угрозой 2021 года в сфере кибербезопасности любой организации, в том числе и финансовой, стал рост числа атак на цепочки поставок. Атаки подобного рода абсолютно не таргетированы. Ключевая цель атаки — компрометация сервисов обновления приложений, которые пользуются доверием корпоративных пользователей, однажды успешно установивших приложение. Зачастую сервисы обновления приложений находятся в доверенной зоне у специалистов по информационной безопасности, поэтому вирусы могут достаточно легко проникнуть в инфраструктуру финансовой организации с очередными обновлениями приложения.

Мощность и длительность DDOS-атак побили в 2021 году все возможные рекорды. Атаки подобного рода чаще всего направлены на дестабилизацию работы инфраструктуры банка. Однако конечным результатом успешной атаки является получение доступа к данным финансовой организации или клиентов на атакуемом объекте. Развитие облачных технологий — одна из причин всё возрастающих размеров проблемы DDOS-атак.

ТАК ЧТО ЖЕ ЖДЁТ ЗАЩИТНИКОВ КИБЕРПРОСТРАНСТВА В 2022 ГОДУ?

С большой долей вероятности можно прогнозировать, что атаки шифровальщиков и нападение на цепочки поставок сохранят свою актуальность. Данные направления кибератак являются высокодоходными для мошенников, а значит, рост масштабов и изощрённости подобного рода атак вполне предсказуемы. Кроме того, в 2022 году нас ждёт

Качественная подделка теперь доступна практически любому злоумышленнику. Звонки от мошенников в роли коллег и руководителей финансовой организации станут новой реальностью, к которой многие банковские структуры пока не готовы. Ведь на сегодняшний день действенной защиты от дипфейка не существует

новая большая проблема — дипфейк. Конечно, абсолютно новым назвать это явление сложно, однако его масштаб в наступившем году существенно вырастет. Одним из вероятных направлений развития этого вида мошенничества является социальная инженерия. Совершенствование технологий подделки голоса и видео вышло сегодня на совершенно новый уровень, и качественная подделка теперь доступна практически любому злоумышленнику. Звонки от мошенников в роли коллег и руководителей финансовой организации станут новой реальностью, к которой многие банковские структуры пока не готовы. Ведь на сегодняшний день действенной защиты от дипфейка не существует.

Вообще, доходы мошенников, полученные путём социальной инженерии в 2021 году, опять побили все возможные рекорды. На текущий момент регуляторы проводят мероприятия, направленные на снижение проблемы социнженерии, но пока это скорее борьба с последствиями, а не с причиной. Пример — предотвращение звонков с подменных номеров. Эти номера добавляют в базы, предупреждая таким образом пользователей. Однако самой проблемы эта мера не решает, и рост числа звонков продолжается. Решением может стать регулирование IP-телефонии. Сейчас эта область очень слабо регулируется, что предоставляет мошенникам пространство для неправомерных действий.

Как уже отмечалось, многие работодатели за пару последних лет вкусили удобство и экономическую выгоду от работы своих сотрудников в удалённом формате. Именно удалёнка останется ключевым трендом, определяющим

развитие технологий в 2022 году. Сервисы видео-конференц-связи, облачные технологии, спрос на мобильность будут развиваться ещё большими темпами. Если говорить о финансовой отрасли, здесь стоит ожидать дальнейшего развития числа атак мошенников на сервисы ДБО, а значит, через них — на инфраструктуру конечных финансовых организаций. Одним из элементов защиты видится развитие технологий многофакторной аутентификации: СМС, PUSH, дополнительные вопросы, капча, FaceID и отпечатки пальцев. Буквально — чем больше факторов, тем лучше. Но все мы понимаем, что зачастую организации боятся «перегрузить» клиента проверками. Действительно, усиление защиты должно сопровождаться облегчением способов подтверждения и обязательно повышением осведомлённости пользователей. Радует, что многие производители оборудования и ПО начинают всё шире использовать данные им возможности в части аутентификации пользователя.

* * *

В заключение хочется отметить, что в нынешних условиях проблема развития информационной безопасности выходит на первый план. Только в РФ ожидается рост затрат на ИБ более чем на 50%, а по миру в некоторых случаях более чем в два раза. Отрадно, что информационная безопасность начинает наконец-то превращаться из «расходного» подразделения в подразделения со своей бизнес-задачей и становится такой же бизнес-функцией, как и многие другие.



Вячеслав ПОЛОВИНКО
руководитель направления
собственных продуктов
АМТ-ГРУП

ДИОДЫ ДАННЫХ

ЭФФЕКТИВНЫЕ СРЕДСТВА ЗАЩИТЫ СЕТЕЙ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Наиболее разрушительные современные атаки на финансовый сектор имеют целенаправленный и многоступенчатый характер. Их успех во многом определяется наличием технической возможности организовать канал удалённого управления системой-жертвой. Эффективный способ исключения несанкционированного доступа злоумышленников к сети — это её надёжная сегментация, то есть выделение в общей сетевой инфраструктуре критических сегментов с их последующей гарантированной изоляцией. Как правило, в финансовых организациях к критическим сетевым сегментам относят: сетевые сегменты размещения АРМ Банка России (АРМ КБР), сегменты размещения АРМ дистанционного банковского обслуживания (АРМ ДБО) с банками-корреспондентами, сегменты выполнения операций процессинга, сегменты хранения резервных копий, сегменты с различными внутренними ИТ-системами, сегменты площадок ведения разработки и тестирования, сегменты размещения продуктивных систем. То есть все те сегменты, доступ к которым извне недопустим ни при каких обстоятельствах.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ

Для решения задач гарантированной изоляции сетевых сегментов многие финансовые организации применяют физическую изоляцию, разделяя сегменты сети между собой «воздушным зазором», в то время как перемещение данных между сегментами допускается лишь с исполь-

зованием учтённых съёмных носителей. Такой подход, наряду с очевидными достоинствами с точки зрения безопасности, имеет ряд недостатков: он исключает возможность передачи данных в реальном времени, затрудняет автоматизацию бизнес-процессов и влияет на непрерывность бизнеса, несёт дополнительную трудоёмкость, провоцирует эксплуатирующий персонал на создание скрытых соединений между сегментами, использование неучтённых носителей информации и нерегламентированных каналов коммуникации. Использование традиционных межсетевых экранов (Firewall) опирается прежде всего на программные решения. Однако даже при самом тщательном тестировании программные продукты подвержены уязвимостям, а наличие двунаправленного канала априори даёт возможность планировать и развивать атаку на банк предметно и долгосрочно. К сожалению, практика показывает, что обновления и патчи безопасности для ПО всё чаще не успевают за угрозами и не могут служить надёжным средством защиты.

ФИЗИЧЕСКАЯ ИЗОЛЯЦИЯ — ГАРАНТИЯ ЗАЩИТЫ

Внедрение устройств однонаправленной передачи данных в банковскую сетевую инфраструктуру устраняет указанные выше ограничения, сохраняя возможность передачи данных между сегментами сети в одном направлении и обеспечивая при этом «воздушный зазор» в обратном направлении. Устройства класса «диод» изолируют сетевые сегменты банка, исключая возможность организа-

ции обратного (в том числе двунаправленного) соединения на физическом уровне и обеспечивая гарантированную защиту сегмента от внешних информационных атак по сети. Таким образом, сегментация банковской сети с применением аппаратных средств позволяет надёжно отделить критические сегменты от остальной сети передачи данных и одновременно обеспечить необходимые взаимодействия между сегментами.

Рассмотрим некоторые возможные сценарии сегментации банковской сети с использованием однонаправленных шлюзов для повышения уровня защиты сетевого периметра.

ЗАЩИТА ПДн

Одной из важнейших задач для банков является защита персональных данных своих клиентов и данных о транзакциях. В то же время в рамках различных бизнес-процессов требуется ограниченный доступ к защищённому сегменту, содержащему эти данные. В ряде случаев требуется исключить возможность компрометации закрытого сегмента сети со стороны внешних подразделений и сотрудников и при этом обеспечить возможность пользоваться обезличенными данными из этой сети. Например, вариант такой организации функционирования контакт-центра банка (или его части), при котором сотрудникам контакт-центра предоставляется доступ к актуальной и, при необходимости, частично обезличенной информации из клиентской базы, но исключается любое воздействие на продуктивную систему банка, ограничивается доступ операто-

ров к более полной информации из баз данных. Обеспечение безопасности и конфиденциальности данных в данном случае обеспечивается путём периодической выгрузки обезличенных данных из продуктивного сегмента через однонаправленный шлюз. Такой сценарий позволяет в принципе ликвидировать возможность атаки со стороны менее доверенного сегмента в случае использования контакт-центра на аутсорсинге.

ОБНОВЛЕНИЕ ИС

Периодическое **обновление информационных систем** банка, в том числе обновление средств защиты информации, например, антивирусных баз и баз репутации, непосредственно сказывается не только на непрерывности, но и на безопасности бизнеса и является жизненно необходимым. Чтобы обеспечить обновления информационных систем, необходимо обеспечить передачу дистрибутивов и образов ПО в продуктивный контур, при этом требуется гарантированно отделить сегмент разработки ПО от продуктивной среды банка. Не секрет, что банки привлекают большое количество внешних команд-разработчиков для эффективного и быстрого развития своей ИТ-инфраструктуры, которые выполняют разработку, тестирование ПО в своей среде разработки. После внешнего тестирования осуществляется загрузка этого ПО в продуктивный или предпродуктивный сегмент банка. Чтобы исключить по этому же каналу риск утечки данных (в том числе и персональных данных клиентов) в сегмент разработки, а также устранить возможность воздействия на продуктивные системы со стороны внешних подразделений и сотрудников, передача файлов обновлений и дистрибутивов может выполняться через однонаправленный шлюз, который физически изолирует один сегмент от другого. В том числе таким образом в закрытый сегмент могут поступать репутационные и антивирусные базы, которые должны постоянно быть актуальными, или файлы обновлений операционных систем.

ДОСТАВКА ДАННЫХ И АНАЛИТИКИ

Доставка информации от новостных агентств в защищаемый сегмент.

Зачастую требуется доставить в защищаемый сегмент банка информацию от новостных агентств (таких как Reuters, Bloomberg и др.), биржевых площадок, размещённых в сети Интернет или в отдельных VPN-сетях. Учитывая высокую ценность работы банковских аналитиков и значимость данных, с которыми они работают, организации требуется исключить утечку данных из сегмента АРМ-аналитиков, которые имеют доступ к данным во внутренних бизнес-системах, и исключить какое-либо воздействие со стороны менее доверенных сетевых сегментов на сеть банка. Размещение однонаправленного шлюза на границе сегмента АРМ-аналитиков и внешнего сегмента (например, Интернет) гарантирует невозможность утечки конфиденциальной информации, а также предотвращает кибератаки, основанные на двунаправленном взаимодействии. При этом сохраняется возможность получения актуальной информации из внешних источников, находящихся за пределами банковской сети.

ХРАНЕНИЕ РЕЗЕРВНЫХ КОПИЙ

Сохранение резервных копий на изолированный ресурс является своего рода страховкой на случай возникновения критических инцидентов в банковской инфраструктуре. Как следствие, важной задачей является сохранение изолированных резервных копий данных и систем с заданной периодичностью и в автоматическом режиме и исключение возможности компрометации данных и самих ленточных хранилищ. Для решения этой задачи необходимо отделить сегмент хранения резервных копий систем банка от остальной сети и гарантированно исключить воздействие на него извне. В случае применения однонаправленного шлюза и передачи резервных копий через него исключается риск атаки на хранилище резервных копий как со стороны открытых сетей передачи данных, так и со стороны скомпрометированного в результате атаки злоумышленника продуктивного контура банка.

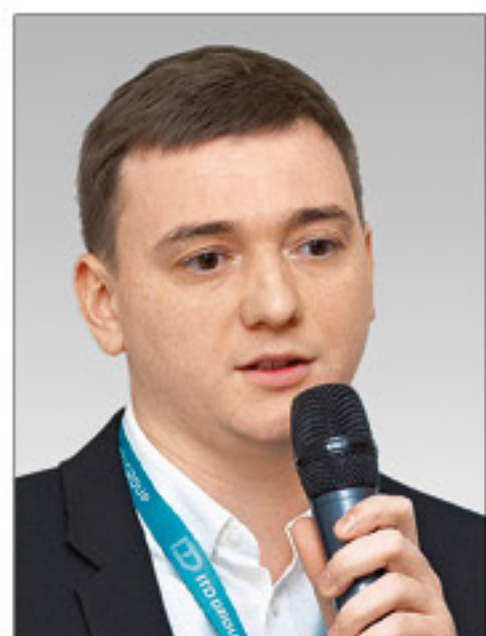
МОНИТОРИНГ СЕТИ СПЕЦИАЛИСТАМИ СОС

Мониторинг состояния сети и информационных систем банка — по-

вседневная и непрерывная задача. Параметры функционирования систем и сети банка или финансовой организации требуют контроля как со стороны служб поддержки, так и со стороны подразделений ИБ, например со стороны СОС, расположенного, как правило, в отдельной подсети банка. В ряде случаев, например для анализа киберинцидентов, требуется привлекать дополнительные, внешние по отношению к банку, организации: экспертов по информационной безопасности, специализированные компании и т.п. Передача и обмен данными во всех указанных случаях предполагает сопряжение двух и более сегментов: продуктивного и менее доверенных. В частном случае передача событий и данных из защищаемого сегмента может происходить, например, с использованием syslog и netflow, а также файлового потока. Передача трафика для регулярного анализа специалистам безопасности через «диод» позволяет обеспечить доставку информации до целевой системы СОС в одностороннем порядке. При этом исключается внешнее воздействие на продуктивный сегмент сети банка в случае, если подсеть ИБ или внешних экспертов сопрягаются с внешними сетями и серверами в целях обновления продуктов ИБ, получения сигнатур вирусов, баз репутации и т.п.

* * *

На сегодняшний день наблюдается расширение сценариев применения систем однонаправленной передачи данных для реализации более эффективных мер защиты периметра финансовой организации. В статье рассмотрены лишь некоторые сценарии: сегментирование сетей в целях защиты персональных данных, организация хранилища резервных копий, удалённый мониторинг и передача данных в СОС и подразделениям ИБ, взаимодействие с вендорами ПО и т.д. Однако на практике количество таких сценариев увеличивается при внимательном отношении к сегментации сети конкретного банка и с учётом актуальной для организации модели угроз.



Александр ЩЕТИНИН
генеральный директор Xello



Владимир СОЛОВЬЁВ
руководитель направления
внедрения средств защиты
АО «ДиалогНаука»

ТЕХНОЛОГИЯ ОБМАНА

ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ DECEPTION

Защищённость корпоративной сети организации — одна из ключевых задач специалиста по информационной безопасности. Если не уделять должного внимания противодействию атакам, то корпоративная сеть становится интересной для злоумышленника, ведь для проникновения в неё не нужно прилагать множества усилий и можно добраться до цели без особых преград.

Сегодня есть множество решений для обеспечения защиты: многие компании строят свои ситуационные центры информационной безопасности (SOC) или используют коммерческие, внедряют «песочницы», используют интеллектуальные межсетевые экраны, проводят аудиты и т.д. Однако все эти меры не гарантируют полную защищённость организации — нападения неизбежны, и нужно уметь чётко понимать, каковы могут быть последствия для организации в случае успешного нападения.

С середины 2020 года существенно увеличилось число различных атак, которые отчасти связаны с тем, что многие организации не были готовы к удалённой работе сотрудников. Сотрудники столкнулись с перебоями в подключении к корпоративной сети, не были готовы к использованию удалённых рабочих мест, VDI, быстрого масштабирования корпоративных облаков и т.д. — и это лишь малая часть причин, которые подтолкнули директоров по информационной безопасности к пересмотру стратегии защищённости организации. Не менее важной причиной является дефицит профессиональных кадров в сфере информационной безопасности.

Согласно последнему исследованию американской компании IDG по приоритетам безопасности, 32% компаний начали внедрять в своих организациях технологию Deception. Это связано с тем, что технологии злоумышленников в развитии целенаправленных атак (APT-атак)

динамично развиваются и тем самым специалисты по всему миру понимают, что защитные меры должны быть соответствующими и опережающими.

КАК ДЕЙСТВУЕТ ЗЛОУМЫШЛЕННИК ПРИ ЦЕЛЕНАПРАВЛЕННЫХ АТАКАХ?

Мошенники продолжают использовать уникальные технологии и методы социальной инженерии для проникновения в корпоративную сеть организации. Проникая во внутренний контур, они в основном используют стратегию замедленного действия, то есть перед каждым следующим шагом происходит оценка рисков и принимается решение о дальнейшем ходе событий. Это позволяет быть незамеченным в инфраструктуре, обойти системы мониторинга и добраться до цели. Важно также учесть, что если злоумышленник прошёл периметровые средства защиты и смог закрепиться в сети в обход систем защиты конечных узлов, то дальше его уже обнаружить крайне сложно без специализированных решений.

КАК ЗАПУТАТЬ ЗЛОУМЫШЛЕННИКА?

Представим ситуацию, когда злоумышленник бесследно проник в сеть и закрепился на любом конечном узле внутри. Решения класса SIEM, NGWF в нужный момент его не обнаружили, и, по сути, компания не знает о проведении атаки. В этом случае поможет технология Deception: она сможет как предотвратить злонамеренные действия, так и в нужный момент оповестить ответственных сотрудников о проникновении

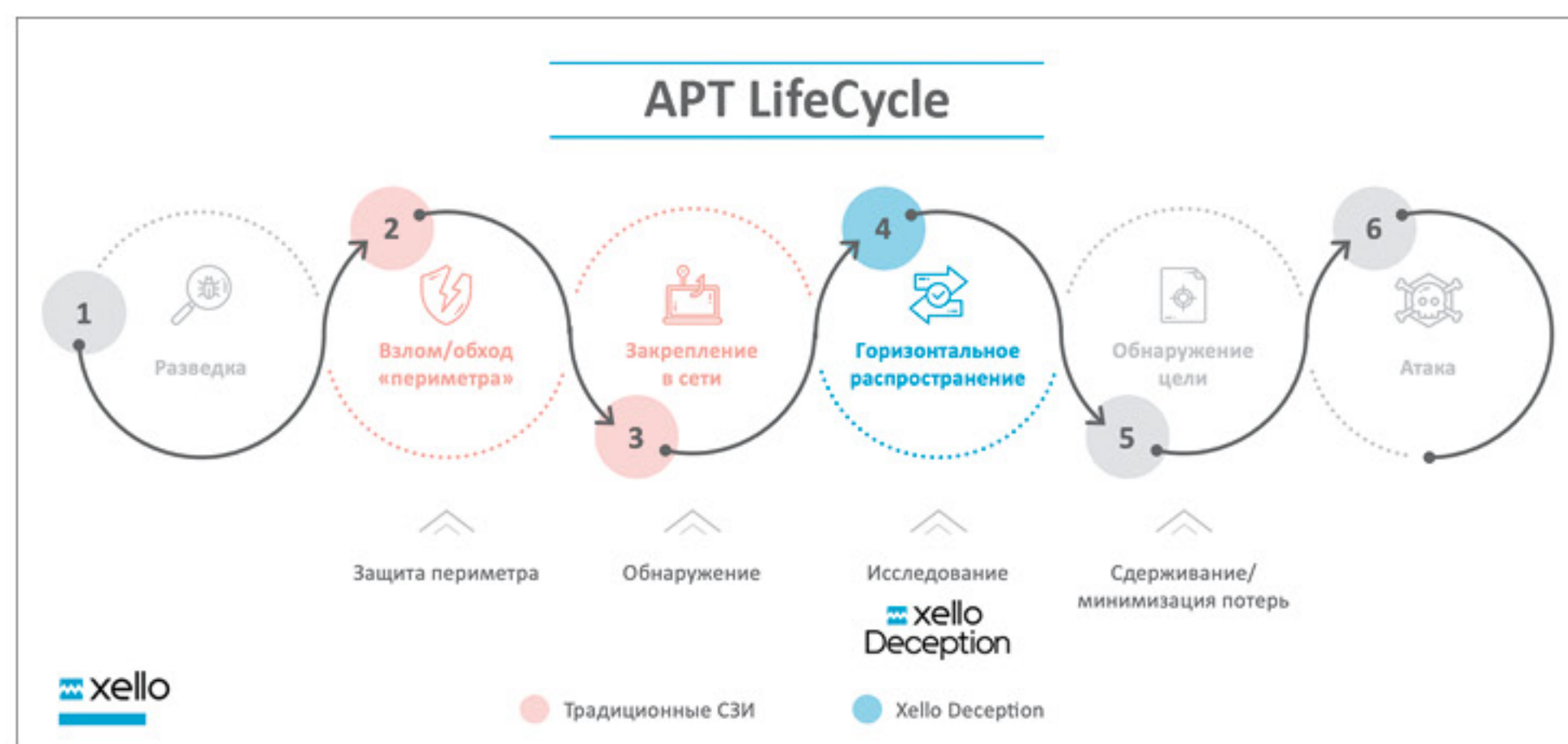


Рисунок 1. Технология Deception может как предотвратить злонамеренные действия, так и оповестить ответственных сотрудников о проникновении во внутренний контур

злоумышленника во внутренний контур (рис. 1). Решение автоматически анализирует структуру и состав Active Directory для того, чтобы на основании анализа создать подходящие приманки и ловушки в виде «ложных» учётных записей, ведущих на несуществующие сервисы, запутывая тем самым мошенника. Deception усложняет задачу нежданному гостю, служит последним рубежом защиты для компании и моментально уведомляет об аномалиях, а также о том, где находится сейчас мошенник и какие осуществляет действия.

ЗАЩИТА С ПОМОЩЬЮ XELLO DECEPTION

Технология продукта Xello Deception уникальна тем, что она не делает точную копию инфраструктуры, а симулирует похожую по синтаксическим признакам. При внедрении и далее в ходе всего цикла использования система непрерывно проводит анализ состава DNS и Active Directory на предмет изучения реальных информационных активов корпоративной сети и на основании полученных данных генерирует приманки и ловушки. Затем приманки, которые злоумышленник не сможет распознать, распространяются безагентским способом на реальные конечные узлы в инфраструктуре организации.

Продукт Xello использует генерацию множества приманок и ловушек, которые имитируют конечные узлы, программное и аппаратное обеспечение, неотличимое от их реальных аналогов в сети. Как только злоумышленник проникает через периметр сети, он проводит разведку, чтобы составить карту сети, и начинает двигаться в сторону обнаружения потенциальной цели. Сеть, содержащая ложные приманки или искусственно созданный трафик, предоставляет злоумышленнику заманчивые цели в виде учётных данных, необходимых для доступа к другим сетевым сегментам.

Эти приманки приводят злоумышленников к ловушкам, имитирующим физические устройства, такие как серверы или отдельные рабочие станции. По мере того как злоумышленник продвигается дальше по пути приманок, технология Xello Deception продолжает свою работу, позволяя злоумышленнику устанавливать вредоносное ПО в ловушки,

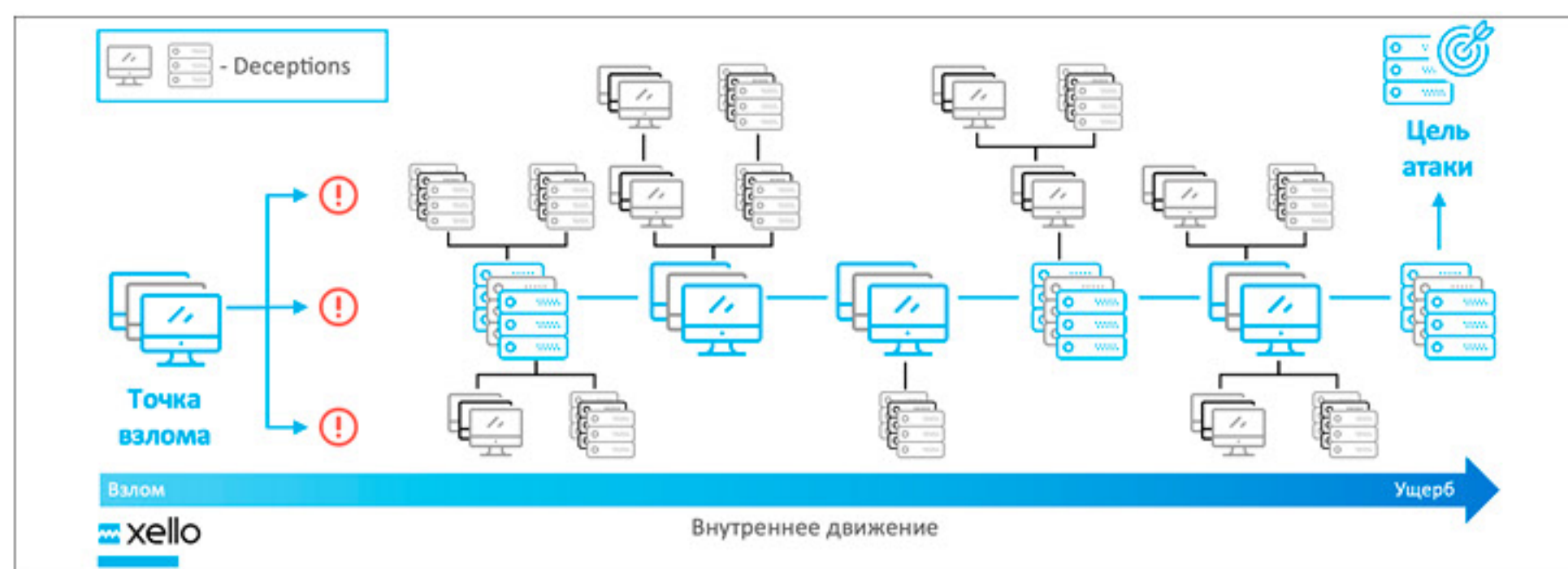


Рисунок 2. Система Deception превращает каждый ПК в ловушку, которой нельзя избежать

создавая иллюзию успешной атаки и одновременно изолируя вредоносное ПО от реальной сети. Продукт позволяет реализовать ловушки в масштабе предприятия, которые смогут обеспечить точный перехват злоумышленника (рис. 2).

При взаимодействии злоумышленника с приманками и ловушками Xello Deception автоматически предупреждает специалистов по информационной безопасности об инциденте и о том, где сейчас находится мошенник и что он сейчас делает, — достаточно лишь зайти в консоль управления в веб-интерфейсе. Быстрое реагирование поможет сократить время нахождения угрозы/злоумышленника в сети организации. Информация о нахождении злоумышленника поможет в дальнейшем понять, какая цель была перед ним, и тем самым усилить защиту данного актива.

Продукт управляется через единую консоль, с помощью которой можно настроить регулярность обновления динамических приманок, ловушек, дополнительных функциональных модулей, проводить мониторинг инцидентов и корректировать события информационной безопасности. Также благодаря Xello Deception можно сократить ресурсы на сбор форензики за счёт регулярного встроенного механизма сбора и анализа данных.

DECEPTION ИЛИ HONEYPOT

Зачастую эти технологии кажутся многим специалистам по информационной безопасности схожими, но хочется прояснить существенную разницу между технологиями Honeypot и Deception:

♦ Honeypot — пассивный инструмент обмана. Ловушки размещаются в сети и не являются динамичными. Злоумышленнику не составит труда их

распознать, поэтому концепция не прижилась на мировом рынке;

♦ Deception — проактивный обман. Приманки меняются динамически, моделируя реальные имена, учётные записи, ключи аутентификации, конфигурационные файлы критичных систем и т.д., благодаря чему максимально похожи на реалистичные данные об инфраструктуре для злоумышленников. К примеру, серверы-ловушки в Xello (TrapServers или High Interactive Honeypot) в этой парадигме — это лишь часть общей экосистемы обмана, которая является лишь одним из множества встроенных средств детектирования.

В частности, в нашей Deception-системе есть кейс, когда не используются серверы-ловушки, а детектирование инцидентов происходит только через ложные данные и корреляцию аутентификационной информации с единого центра аутентификации, например Active Directory. Это далеко не единственный пример, но очень показательный, который всегда отвечает на вопрос «в чём ваше отличие от классических honeypot и чем вы лучше?».

ВМЕСТО ЗАКЛЮЧЕНИЯ

Технология Deception признана Gartner как одна из перспективных. Российский рынок, как и зарубежный, с интересом смотрит на технологию и активно тестирует новинку. Сценарии использования во многих компаниях разные: кто-то применяет продукт при проведении тестирования на проникновение или Red Team и тем самым повышает качество проведения аудитов, кто-то до конца не понимает, что происходит в сети, и хочет понять ситуацию, а у кого-то были инциденты и важно не допустить новых. Тестируйте новые технологии и защищайтесь от инцидентов по-новому!

**Дмитрий НАГИБИН**

руководитель департамента
разработки средств защиты
станций и серверов Positive
Technologies

PT XDR СНИМАЕТ БОЛЬ ИНДУСТРИИ

И СОЗДАЁТ ЕДИНЫЙ КОНТЕКСТ СОБЫТИЙ ИБ
И УСКОРЕННОЕ РЕАГИРОВАНИЕ НА АТАКИ

Под занавес 2021 года Positive Technologies представила рынку новое решение для качественного обнаружения киберугроз и реагирования на них, относящееся к классу XDR¹, — PT XDR, а также его финальный элемент для защиты конечных точек PT EDR. В чём сила позитивного XDR, как решение помогает специалистам по кибербезопасности реагировать на атаки и почему PT XDR нужен бизнесу?

Индустрия кибербезопасности в мировом масштабе не справляется с актуальными вызовами и не в состоянии гарантировать невозможность реализации недопустимых для бизнеса событий. Проблема кроется в том, что отрасль поставляет средства защиты, которые могут быть хороши и эффективны только в отдельно взятой области, как разрозненные запчасти, в то время как задача по «сборке автомобиля» остаётся на стороне компаний. За десятилетия организации не научились складывать пазл целиком, что подтверждается результатами сотен пентестов, проводимых Positive Technologies. И мы не видим в этом ничего удивительного: вернёмся к метафоре с автомобилем — мало кто сможет собрать его даже из самых лучших запчастей. Мы осознали данную парадигму ещё три года назад и

считаем, что ответственность «по сборке ИБ» в компаниях должна перейти к поставщикам решений и сервисов. Поэтому мы задались целью создавать продукты, позволяющие обнаружить и остановить злоумышленников до того, как они причинят компании непоправимый ущерб, и демонстрируем реальность результативного подхода к кибербезопасности, подразумевающего гарантии невозможности реализации самых негативных для бизнеса сценариев, которые потенциально можно осуществить через IT-инфраструктуру в результате кибератаки.

Решение PT XDR позволяеткратно ускорить реагирование на атаки и является неотъемлемой частью наших метапродуктов (в частности, MaxPatrol O2), которые направлены на автоматическое обнаружение и предотвращение действий злоумышленников в корпоративной инфраструктуре, в идеале — силами одного специалиста.

В ЧЁМ ПОЛЬЗА XDR-СИСТЕМ

Сегодня каждый инцидент так или иначе затрагивает рабочие станции: профессиональные киберпреступники используют многовекторный подход для проникновения в корпоративную сеть и атакуют максимальное количество элементов инфраструктуры. Поэтому организациям важно одновременно отслеживать потенциальные точки проникновения и оперативно устанавливать

взаимосвязи между событиями на этих точках.

XDR-системы позволяют получить полную картину происходящего в инфраструктуре за счёт собственных агентов и сетевых сенсоров, а также за счёт объединения продуктов (о них далее) в единую среду обмена данными. Решения этого класса помогают выяснить причины заражения либо компрометации и предпринять верные действия по реагированию.

Набор средств защиты в составе XDR изменяемый: он может, например, собирать информацию с таких систем, как EDR², NDR³, SIEM⁴, Sandbox⁵, WAF⁶ и VM⁷. За счёт сбора событий с разных продуктов в единый контекст XDR-решение предоставляет аналитикам в одном интерфейсе всю необходимую информацию об атаке и весь требуемый инструментарий для реагирования, что сокращает время на поиск и блокирование угроз, причём в рамках всей инфраструктуры, а не отдельных её элементов. Системы класса XDR, позволяющие частично автоматизировать рутинную работу SOC-подразделений, в первую очередь необходимы крупным

² Endpoint detection & response

³ Network detection and response

⁴ Security information and event management

⁵ Сетевая песочница

⁶ Web application firewall

⁷ Vulnerability management

¹ Extended detection and response, расширенное выявление угроз и реагирование на них

компаниям для противодействия сложным киберугрозам.

СИЛА XDR

Появление новых способов защиты вызывает у киберпреступников ответные действия — они начинают искать варианты её обхода. И наоборот, ранее неизвестные инструменты злоумышленников мотивируют специалистов по кибербезопасности начать поиски новейших возможностей по защите. С появлением PT XDR, а вместе с ним EDR-решения мы можем доносить до «эндпоинтов» знания о том, как атакующие взламывают системы. XDR — это инструмент, который позволяет проверять гипотезы компрометации на реальной сети агентов и на основании собранной телеметрии пытаться искать атаки, которые были ранее неизвестны. Мало примеров на рынке ИБ-решений, даже в других классах, которые позволяют реализовать данный подход, в PT XDR это достигается за счёт объединения телеметрии из разных источников, мы логируем не только то, что считаем подозрительным, а даже легитимные действия процессов в ОС, чтобы потом иметь возможность восстановить всю картину целиком и на основе большего объёма данных их скоррелировать и выявить ранее неизвестный вектор атаки.

Мы знаем, как злоумышленники атакуют компании по всему миру, поэтому понимаем, как от них защищаться. При разработке любого своего продукта мы опираемся на свой многолетний опыт по обнаружению реальных атак и расследованию инцидентов, а также по нахождению уязвимостей. Эти знания наши продукты получают от двух команд Positive Technologies — исследовательского центра PT SWARM и экспертного центра безопасности (PT Expert Security Center). Специалисты последнего постоянно отслеживают активность хакерских группировок (в том числе и ранее неизвестных), действующих на территории России и мира, и могут по первым признакам и с высокой точностью определить, какая группировка стоит за конкретным инцидентом. А команда PT SWARM, в свою очередь, делает технологическую среду безопаснее: за последние три года эксперты выявили более 250 уязвимостей, 70% из

которых высокого и критического уровня опасности, в программных продуктах 60 различных производителей. Все эти знания мы передаём в наши продукты.

PT XDR аккумулирует технологии продуктов Positive Technologies (PT Sandbox, MaxPatrol SIEM, MaxPatrol VM, PT NAD, PT ISIM, PT Application Firewall и PT EDR), что позволяет как коррелировать события безопасности на конечных узлах, так и поднимать необходимый контекст вверх, чтобы устанавливать соответствия, выявлять действия злоумышленников, обнаруживать дополнительные инциденты, которые до этого находились в слепой зоне, и реагировать на них в автоматическом режиме намного раньше, чем наши продукты могли это сделать прежде. Также PT XDR позволяет обогащать уже сформированные, переданные или записанные инциденты.

О СКОРОСТИ РЕАГИРОВАНИЯ И ПРЕИМУЩЕСТВАХ АВТОМАТИЗАЦИИ

Получение максимального контекста в кратчайшие сроки и с минимальными трудозатратами специалистов — это основная потребность компаний, стремящихся нивелировать риски и испытывающих дефицит в экспертах. При этом именно скорость реагирования на угрозы называют главным параметром, позволяющим повысить защищённость бизнеса. Поиск и анализ угроз занимает у аналитика SOC время, так как ему приходится одновременно работать с большим числом средств мониторинга и защиты, смотреть во множество консолей. А время — самый ценный ресурс: чем дольше специалист по ИБ пытается понять, что происходит и как на это отреагировать, тем больше шансов у хакеров закрепиться в инфраструктуре. Если говорить о конечных точках, то колоссальное значение имеет детектирование действий на рабочих станциях (скорость перемещения злоумышленников по ним измеряется минутами), а также умение отличить их от активности авторизованных пользователей. Злоумышленники очень часто используют легитимный инструментарий, который есть в инфраструктуре, в своих целях.

Отслеживание защищённости корпоративной инфраструктуры в интерфей-

се одной системы невозможно реализовать без удобного инструмента. PT XDR позволяет операторам SOC всегда иметь целостное представление об инфраструктуре и степени её защищённости, а также о безопасности устройств. Решение даёт возможность почти молниеносно реагировать на кибератаки (в том числе на конечных точках) — скорость реакции измеряется секундами. С помощью PT XDR специалисты по кибербезопасности могут выявить угрозу как на начальном этапе, когда атака только начала развиваться, и сразу же заблокировать эксплуатацию уязвимости или любую другую вредоносную активность на скомпрометированном узле, так и на этапе, когда злоумышленники уже успели развить атаку внутри инфраструктуры. Специалисты по ИБ получают более качественное обнаружение вплоть до причины заражения, что позволит обеспечить новый уровень безопасности с учётом обогащённой информации.

PT XDR решает основную боль индустрии — нехватку квалифицированных кадров на рынке. Мы снижаем требования к компетенции специалистов по ИБ и их числу в штате SOC за счёт того, что передаём недостающую экспертизу через наши продукты. Кроме того, наше XDR-решение позволяет автоматизировать процесс реагирования на киберугрозы: не дожидаясь действий оператора, продукт может самостоятельно принимать решение по блокировке атак, остановке подозрительных IT-процессов или перемещению файлов в карантин — в общем, делать всё, чтобы не позволить свершиться недопустимым для бизнеса событиям.

* * *

Коммерческая версия PT XDR станет доступна во II квартале 2022 года. Прямо сейчас можно подать заявку на участие в программе Early birds и записаться на проведение «пилота» на собственной IT-инфраструктуре. Преимущество раннего тестирования решения состоит в том, что Positive Technologies будет расширять список собираемой информации и автоматизировать сценарии реагирования, релевантные именно вашей инфраструктуре.



Дмитрий ГУСЕВ
заместитель генерального
директора компании
«ИнфоТеКС»

ИМПОРТОЗАМЕЩЕНИЕ В КРЕДИТНО-ФИНАНСОВОЙ ОТРАСЛИ

РЕАЛИИ И ПЕРСПЕКТИВЫ

Курс на импортозамещение в кредитно-финансовой отрасли был определён как одна из составляющих общей политики импортозамещения в России. Тема эта обсуждается уже не первый год на разных площадках, в том числе и на Уральском форуме. О том, как обстоят дела по части импортозамещения в сфере информационной безопасности, мы беседуем с Дмитрием Гусевым, заместителем генерального директора компании «ИнфоТеКС» — одного из крупнейших производителей средств защиты информации.

— Оказал ли курс на импортозамещение в финансовой сфере влияние на вашу продуктовую линейку?

— Мы всегда старались делать универсальные решения без акцента на конкретную отрасль, но если говорить про финансовую сферу, то у нас есть специализированное решение: платёжный HSM — ViPNet HSM PS, идея разработки которого пришла в момент, когда в России всерьёз заговорили про создание национальной системы платёжных карт (НСПК).

В платёжных системах HSM реализует множество важных криптографических операций при работе с платёжными картами банков и терминалами оплаты: инициализация и персонализация карт, валидация карт и операций

при совершении расчётов, смена параметров карты, например пин-кода и пр. И самое важное — хранение секретных параметров (ключей) карт в неизвлекаемом виде, что гарантирует невозможность подделки платёжных карт.

Работу над платёжным HSM мы начали в 2015 году. Партнёром по этому проекту стала компания «Системы практической безопасности» (СПБ)¹. С этого момента началось наше плодотворное сотрудничество, которое вылилось также в ряд других сервисов и продуктов, например линейку PKI-решений, генератор ключей и профилей для sim-карт и eSIM, а также совместные работы по стандартизации криптографических механизмов.

В 2018 году ViPNet HSM PS получил сертификат соответствия требованиям ФСБ России к СКЗИ по классу КВ. При этом это было первое СКЗИ в России с одновременной поддержкой алгоритмов ГОСТ и зарубежной криптографией, необходимой для обеспечения совместимости с существующими платёжными системами банков.

— Как пришла идея создания отечественного платёжного HSM?

— Тут всё просто: любой разработчик ищет новые рыночные ниши для своих

продуктов, и мы посчитали, что могли бы использовать свой многолетний опыт разработки СКЗИ для создания отечественного аналога аппаратных криптографических модулей (HSM) в интересах как минимум НСПК, призванной обеспечить национальную безопасность, надёжность и бесперебойность розничных платёжных сервисов в условиях осложнения геополитической обстановки². И здесь следует понимать, что HSM является ключевым элементом безопасности любой платёжной системы — это не мои слова, а, по сути, прямой перевод международных требований к платёжным системам³.

Хочу подчеркнуть: чтобы сделать отечественный платёжный HSM, недостаточно просто изготовить «железо» с необходимым набором функций, нужно проверить его корректную работу с платёжными системами, внедрёнными на стороне заказчика.

Разработанный нами ViPNet HSM PS успешно прошёл тестирование на совместную корректную работу на стороне крупнейшего международного разработчика процессинговых решений OpenWay, а позднее и в одном из крупных российских банков. Тестирование

² Стратегия развития НСПК 2019–2021. <https://www.nspk.ru/upload/strategy.pdf>

³ Payment Card Industry PTS HSM Modular Security Requirements, v4.0. Page 1

¹ На сегодняшний день компания «СПБ» входит в группу компаний «ИнфоТеКС»

подтвердило, что в техническом плане наш платёжный HSM не уступает зарубежным аналогам, которые сейчас эксплуатируются во всех платёжных системах, работающих в России, включая НСПК.

— **Что препятствует распространению отечественных HSM?**

— В теме импортзамещения платёжных HSM есть важный момент, который уже несколько лет стопорит внедрение российских разработок, — расхождения в трактовке различными экспертами международных требований и рекомендаций Совета по безопасности платёжных систем (PCI Security Standards Council или PCI SSC). Позволю здесь себе высказать и нашу позицию.

Все международные платёжные системы являются участниками PCI SSC и следуют единым правилам и требованиям этой организации. Таким образом достигается высокий единый уровень безопасности платёжных систем. Перечень требований включает в себя требования к участникам платёжных систем (банкам, операторам платёжных систем), программным и техническим средствам, в т.ч. к POS-терминалам и HSM.

Самый простой и понятный путь прохождения оценки соответствия этим требованиям для любого участника платёжной системы — использование сертифицированных специальными лабораториями (PCI Recognized Laboratories) элементов платёжных систем, включая HSM. И именно этой позиции придерживается большая часть экспертов ИБ из российской банковской сферы. Лаборатории аккредитуются самой PCI SSC, и в России таких лабораторий нет, а перспективы их появления в свете современной геополитики весьма туманны. Также непонятны перспективы сертификации российских СКЗИ в действующих зарубежных лабораториях.

Однако, если внимательно читать документы и декларации на сайте PCI SSC, то из них следует, что обязательность применения в той или иной платёжной системе именно сертифицированных в PCI Recognized Laboratories изделий HSM является рекомендацией

Чтобы сделать отечественный платёжный HSM, недостаточно просто изготовить «железо» с необходимым набором функций, необходимо проверить его корректную работу с платёжными системами, внедрёнными на стороне заказчика

со стороны PCI SSC. Окончательное решение в данном вопросе остаётся за оператором платёжной системы.

Более того, PCI SSC в своих требованиях к участникам процессинга явно оговаривает правила соотнесения этих требований с национальными законодательствами. Приведу следующую цитату из PCI DSS: «...законодательством или нормативно-правовыми актами могут быть предусмотрены особые требования по защите персональных данных или иных элементов данных... Стандарт PCI DSS не заменяет собой местные или региональные законы».

В рамках этой позиции PCI SSC мы уже несколько лет задаёмся вопросом, почему бы российской национальной платёжной системе не иметь свои требования к HSM, копирующие все функциональные требования PCI PTS HSM и соответствующие при этом требованиям ФСБ России к СКЗИ? Оценку же соответствия разработанных в России HSM таким комбинированным требованиям могут проводить действующие российские лаборатории, аккредитованные ФСБ. Это и могло бы стать тем самым решением оператора платёжной системы.

Обсуждение всех этих вопросов на уровне рабочей группы Банка России и НСПК, включая экспертов отрасли, несколько лет назад привели в рамках программы «Цифровая экономика» к организации при НИИ «Восход» лаборатории по тестированию и исследованию оборудования для платёжных систем по требованиям PCI SSC. К сожалению, как я уже отметил выше, перспективы аккредитации этой лаборатории в PCI SSC неясны. Пока лаборатория проводит исследования только с точки зрения функциональности устройств.

Важно, что рабочей группой Банка России с участием экспертов ИнфоТеКС

и СПБ уже подготовлены функционально-технические требования, технологические карты с описанием необходимой функциональности POS-терминалов и платёжных HSM. А в рамках работ Технического комитета по стандартизации № 26 введены в действие методические рекомендации по использованию отечественных криптоалгоритмов при реализации функций платёжных систем.

Несмотря на все сложности, мы с оптимизмом смотрим на перспективы использования в российских сегментах международных систем и в национальной платёжной системе своего HSM.

— **Что может помочь развитию рынка отечественных HSM?**

— Если в России появится лаборатория, аккредитованная на проведение исследований по требованиям PCI SSC, это, конечно, существенно ускорит появление необходимого оборудования. Но пока верится в такое событие слабо.

Не так давно вышло положение ЦБ № 382-П (в текущей редакции 719-П), предписывающее, что с 2024 года в значимых платёжных системах должно использоваться оборудование отечественного производства, реализующее западные криптоалгоритмы. Получается, что с 2024 года использование оборудования зарубежных вендоров должно быть ограничено.

А с 2031 года уже должен быть осуществлён переход на отечественные криптоалгоритмы, при этом оборудование должно быть сертифицировано по требованиям ФСБ России.

— **Какие ещё решения для защиты информации вы готовы предложить финансовым организациям?**

— В соответствии с курсом России на импортзамещение и Законом об автономном устойчивом суверенном Рунете,



Внешний вид модели ViPNet TLS Gateway в виде ПАК (TLS 500/1000) и Web-интерфейс администрирования ViPNet TLS Gateway



Шлюз безопасности ViPNet xFirewall класса NGFW

который был подписан Президентом в мае 2019 года, было принято решение о создании национальной системы маршрутизации трафика и применения отечественных алгоритмов шифрования данных, передаваемых по сетям связи в РФ.

Система должна обеспечить устойчивость и безопасность информационного взаимодействия граждан с информационными ресурсами госорганов по защищенным протоколам с поддержкой российских алгоритмов шифрования. Пока план перехода на отечественные криптоалгоритмы становится обязательным для государственных информационных систем. Возможно, в будущем эта законодательная инициатива распространится и на финансовый сектор, как часть КИИ.

Уже сейчас наша компания готова предложить целый ряд продуктов для организации защищенного доступа с помощью протокола TLS с отечественной криптографией, например, к системам ДБО. Это шлюзы ViPNet TLS Gateway и разнообразное клиентское ПО под разные операционные системы и аппаратные архитектуры с поддержкой TLS ГОСТ. Особо отмечу, что наши шлюзы TLS сертифицированы и поддерживают одновременную работу на отечественной и зарубежной

криптографии, что позволяет заменять ими зарубежные продукты максимально просто, без перенастройки прикладных систем с последующим плавным переходом на ГОСТ по мере замены клиентского ПО.

Выше я рассказывал про наши криптографические решения и продукты, но есть у нас и некриптографические СЗИ: сетевые экраны, системы обнаружения вторжения уровня сети и хоста. Например, наш шлюз безопасности ViPNet xFirewall класса NGFW уже сейчас целым рядом заказчиков используется для замены зарубежных межсетевых экранов, с пропускной способностью до 10 Гбит/с. Работаем и над более производительными моделями.

В своих системах обнаружения вторжения ViPNet IDS мы используем фирменную базу сигнатур атак и эвристики, которые разрабатывает наша дочерняя компания «Перспективный мониторинг». В ней используются как доступные проверенные зарубежные источники сигнатур, так и собственные сигнатуры, разрабатываемые аналитиками SOC Перспективного мониторинга. Эта база регулярно обновляется и пополняется новыми сигнатурами и, на наш взгляд, по своей эффективности не уступает коммерческим зарубежным аналогам.

Есть у нас и бизнес-ориентированные разработки, например наш защищенный мессенджер ViPNet Connect. Это не попытка заменить облачные мессенджеры, будь то всем известные зарубежные системы или менее известные отечественные. Это решение корпоративного класса для организации защищенного обмена сообщениями, файлами, осуществления голосовых и видеозвонков внутри организации или между организациями, когда заказчик хочет контролировать весь информационный обмен, не доверяя его облачным сервисам. В 2021 году мы проводили большую работу по интеграции своего мессенджера с ВКС российских разработчиков: поддержали работу с TrueConf, VideoMost и «Протеом».

Поводя итог, мне остаётся лишь подчеркнуть, что ИнфоТеКС уже давно не только разработчик средств криптографической защиты, а компания, нацеленная на создание и развитие комплексной продуктовой линейки СЗИ, соответствующей всем современным требованиям регуляторов и рынка. И мы надеемся, что наш опыт, разработки и наша готовность учитывать запросы потребителей позволят нам найти в кредитно-финансовой отрасли своих многочисленных заказчиков.



Андрей МУЛЛИН
руководитель группы
решений информационной
безопасности, СТИ

DEVSECOPS. БЕЗОПАСНАЯ РАЗРАБОТКА

ПЕРЕХОД ОТ DEVOPS К DEVSECOPS ОСУЩЕСТВЛЯЕТСЯ
ПРОЗРАЧНО, БЕЗ СУЩЕСТВЕННЫХ ПРОБЛЕМ

Любые нововведения зачастую вызывают противоречивую реакцию: «Зачем? Почему? Для чего?». Можно провести множество аналогий, в том числе переход от разработки по методу Waterfall к Agile, в результате которого процесс становится более эффективным и гибким, благодаря чему результат достигается значительно быстрее.

Одним из таких значительных нововведений было появление методологии DevOps, которая кардинально изменила процесс разработки программного обеспечения. Простая, но революционная методология оказалась эффективной и дала ряд преимуществ для

выпуска высококачественного продукта и активного взаимодействия разработчиков ПО и специалистов, ответственных непосредственно за ИТ-системы.

ПОТРЕБНОСТЬ В ИНТЕГРАЦИИ ИБ И CI/CD

Общая концепция DevOps привела к созданию таких практик, как CI/CD (непрерывная интеграция + непрерывная поставка). Единственным узким местом оказались аспекты информационной безопасности. Взаимодействие с ИБ-специалистами только на финальном этапе вызывает определённые сложности, поскольку для устранения

замечаний и уязвимостей в уже готовом продукте может потребоваться внесение значительных изменений в существующий код. Фактически при устранении выявленных недостатков и проблем в готовом продукте речь идёт о новом цикле процесса разработки, что вызывает негативное отношение со стороны разработчиков, а также может спровоцировать финансовые и репутационные потери. Поэтому возникла потребность в интеграции ИБ и CI/CD для обеспечения непрерывного и прозрачного процесса разработки и выполнения требований по части ИБ на начальных этапах разработки и проектирования решения.

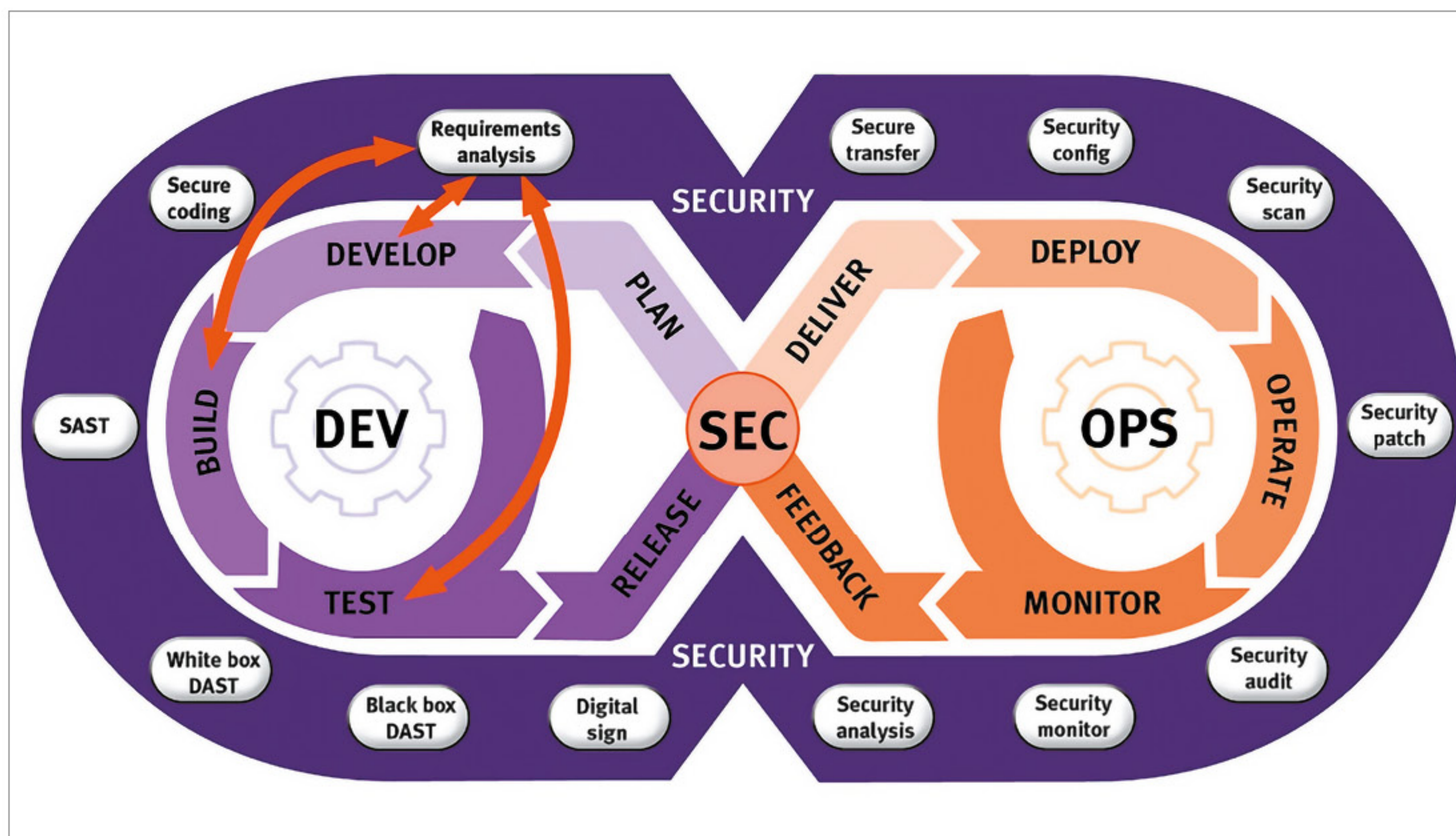


Рисунок 1. Модель процесса DevSecOps (инструменты и методы)

ОСНОВНЫЕ ПРОБЛЕМЫ

DevSecOps — то самое нововведение, цель которого — дополнить эффективный, продуктивный процесс CI/CD необходимыми механизмами обеспечения безопасности. Понятию уже несколько лет, но активно использовать его начали в течение последних двух. Разумеется, как и любое новшество, DevSecOps вызывает определённый скептицизм при рассмотрении. В кругах разработчиков ошибочно фигурирует мнение, что добавление механизмов обеспечения безопасности к процессу CI/CD лишь замедляет его либо стопорит совсем. Давайте разберёмся с основными проблемами, с которыми сталкиваются при внедрении DevSecOps.

1) DevSecOps = набор отдельных решений (см. рис. 1)

Необходимо понимать, что DevSecOps — это расширение DevOps методами обеспечения кибербезопасности (Sec) применительно к процессу CI/CD. Добавление механизмов SCA, SAST, DAST/IAST и CSA к этапам CI/CD подразумевает использование

определённых классов решений, как open-source, так и commercial, но сама суть DevSecOps заключается в обеспечении безопасности процесса CI/CD путём привлечения в команду ИБ-специалистов, а также повышения квалификации разработчиков в контексте компетенций по ИБ.

Для обеспечения необходимой функциональности Sec необходимы следующие решения:

- ♦ решения класса SCA (Software Composition Analysis), обеспечивающие проверку продукта на наличие проблемных зависимостей, такие как WhiteSource, BlackDuck, Sonatype и Snyk;

- ♦ решения класса SAST (Static Application Security Testing), обеспечивающие проверку исходного кода для выявления уязвимостей и проблемных мест, такие как SonarQube, Coverity, Veracode, Checkmarx;

- ♦ решения класса DAST (Dynamic Application Security Testing), обеспечивающие динамическое тестирование безопасности продукта (тестирование методом «чёрного ящика»), такие как Veracode, Acunetix, Burp Suite, Fortify WebInspect, OWASP ZAP;

- ♦ решения класса IAST (Interactive Application Security Testing), обеспечивающие интерактивное тестирование безопасности приложения, сочетая преимущества решений классов SAST и DAST и обеспечивая более высокую эффективность анализа. Мы, эксперты CTI, рекомендуем решения Seeker (Synopsys) и VeraCode;

- ♦ решения класса CSA (Container Security Analysis), которые обеспечивают анализ образов контейнеров на уязвимости и мониторинг их активности. Однозначными лидерами рынка являются решения Palo Alto Prisma Cloud и Aqua Security Cloud Native Security Platform.

2) Назначение DevSecOps, или «Зачем постоянно проверять код, влезать в этапы разработки?»

DevSecOps сейчас активно развивается, это трендовая тема. Связано это с тем, что большая часть компаний финансовой отрасли и ретейла имеет свои команды разработки, которые реализуют интеграционные проекты и собственные продукты. Для этих предприятий вопросы информационной безопасности жёстко регулируются

законодательством. Безопасность разработки и разрабатываемого кода — это не прихоть отдела ИБ, это текущая необходимость и потребность.

На самом деле, если рассматривать процесс разработки как коммерческого, так и собственного ПО, можно смело утверждать, что разрабатываемый код проходит ряд проверок и тестов изначально. Большинство методов, направленных на обеспечение безопасности кода, были известны и применялись ранее, например, использование валидации вводимых данных (input validation). Однако обычных методов недостаточно для выявления уязвимостей как на ранних, так и на поздних этапах разработки. Причины достаточное количество, поскольку используемые приложениями библиотеки могут содержать уязвимости нулевого дня либо иметь ранее не выявленные уязвимости и проблемы как самого кода, так и архитектуры. Необходимо учитывать, что разработка тех или иных приложений включает в себя использование стороннего кода, библиотек и приложений, которые также могут иметь аналогичные проблемы.

Процесс выявления и исправления ошибок и уязвимостей на ранних стадиях разработки выгоден как с позиции затрат (снижение финансовых и временных затрат на устранение недостатков), так и с позиции репутации (отсутствие значительных уязвимостей и проблем в ПО).

Зачастую незнание и непонимание тех или иных принципов, подходов, методов вызывает ряд проблем при появлении перемен и новшеств, что мы наблюдаем при текущей миграции к DevSecOps. Мы однозначно рекомендуем проводить регулярное обучение разработчиков как общим аспектам ИБ, так и аспектам ИБ в области разработки в качестве минимального набора мер. Разработчикам будет проще понять и принять нововведения, если они будут осведомлены о текущих проблемах безопасности и о необходимости её обеспечения. Немаловажным становится и изменение подхода и мышления при разработке, формирование понимания «если сейчас сделаем плохо, будут уязвимости, придётся переделывать».

Процесс выявления и исправления ошибок и уязвимостей на ранних стадиях разработки выгоден как с позиции затрат (снижение финансовых и временных затрат на устранение недостатков), так и с позиции репутации (отсутствие значительных уязвимостей и проблем в ПО)

3) Процесс интеграции с CI/CD, или «Сейчас придут злые безопасники и застопорят нам процесс»

Использование инструментов Sec обеспечивает успешное завершение каждого из этапов разработки за счёт выявления потенциальных проблем и уязвимостей и их предотвращения на ранних стадиях (так называемый сдвиг безопасности влево). Обеспечение безопасности как разработки, так и конечного продукта — это непрерывный процесс, который напрямую отражён в философии Agile. Развитие технологии, методов, паттернов разработки, появление новых языков программирования, библиотек, ОС — всё это сказывается как на самом процессе разработки, так и на процессе обеспечения безопасности. И процесс, и конечный продукт становятся сложнее, что создаёт определённые проблемы при анализе кода и продукта в контексте безопасности.

Как и в любом ИТ-процессе, набор средств, утилит, решений — это только полдела. Анализ исходного кода, дизайн-проекта, готового продукта автоматизированными средствами не обеспечивает 100 %-й защищённости. Нюансы композиции, архитектуры, компонентов могут быть решены только профессиональным анализом со стороны профильных специалистов в области информационной безопасности (например, AppSec-инженеров) при условии полноценного погружения в проект, начиная с самых ранних этапов. Этот момент возможен только при проактивной, совместной работе всех участников проекта, при которой заранее определены зоны ответственности, обязанности и регламент взаимодействия между участниками.

Таким образом, грамотное построение процесса взаимодействия Sec и

DevOps-команд при внедрении практик DevSecOps является одним из самых важных моментов во всей методологии. Обеспечение безопасности не должно вызывать нарушения в процессе CI/CD или конфликтные ситуации между участниками. Специалисты Gartner в публикации «12 Things to Get Right for Successful DevSecOps» (публикация G00450792 от 19.12.2019) дали ряд рекомендаций, как этого достигнуть:

- ♦ добейтесь плавной интеграции механизмов и методов обеспечения безопасности и соответствия требованиям в DevSecOps без нарушения или прерывания текущих процессов для непосредственных участников (разработчиков);

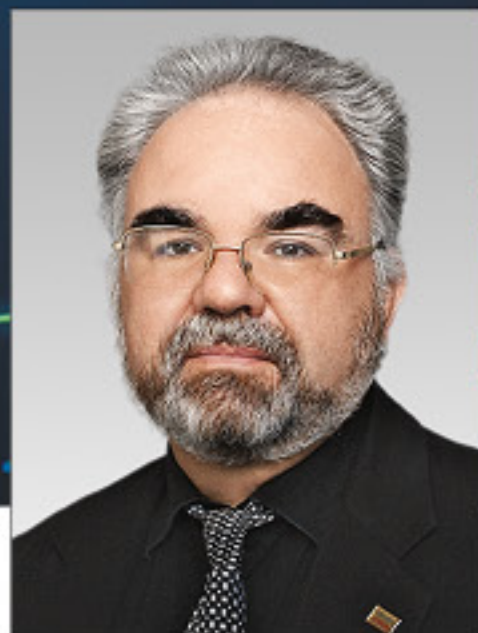
- ♦ сосредоточьте внимание на критичных подтверждённых проблемах и уязвимостях, не пытаясь устранить все неизвестные уязвимости (которые могут вызвать ложноположительные срабатывания на тестах);

- ♦ используйте новые типы инструментов и подходов, таких как интерактивное тестирование безопасности приложений, для обеспечения удобства разработчиков;

- ♦ повышайте квалификацию и осведомлённость разработчиков в области информационной безопасности.

* * *

В целом, при должном планировании, грамотном подборе технических средств и решений, поэтапной миграции и, прежде всего, активной коммуникации между участниками переход от DevOps к DevSecOps осуществляется прозрачно, без существенных проблем. Но если они возникнут, эксперты СТИ готовы вам помочь.



Алексей ЛУКАЦКИЙ
эксперт BIS Journal

SOC-ФОРУМ 2021

«SOC НЕ УМЕРЛИ, ЧТО БЫ НИ ГОВОРИЛИ НА ЗАПАДЕ»

В начале декабря в Москве при большом скоплении народа прошёл традиционный слёт тех, кто занимается центрами мониторинга и реагирования на инциденты ИБ, — SOC-Форум 2021, который продемонстрировал, что между взглядами на SOC в России и на Западе наметилось серьёзное расхождение. И я даже не говорю про достаточно радикальную позицию «SOC мертвы», которая нередко звучит на западных мероприятиях. Речь идёт о совершенно другом: западный рынок ИБ очень активно движется

в облака, и направление SOC не является исключением. Кроме того, западный мониторинг ИБ и реагирование на инциденты неразрывно связаны с автоматизацией, а где-то уже и с low code / no code, о которых у нас тоже пока говорят на мероприятиях не очень активно. Но, с другой стороны, ввиду грядущего железного занавеса и всё более реального шанса нарваться на санкции, которые сделают многие зарубежные инновации для нас недоступными, может, и не стоит ориентироваться на то, что делают наши зарубежные партнёры?

ГОССОПКА ПОВОРАЧИВАЕТСЯ ЛИЦОМ

Прошедший SOC-Форум стал первым, на котором представители НКЦКИ не просто рассказывали очевидные вещи о том, как взаимодействовать с ГосСОПКА, а представили аналитику — динамику угроз ИБ за последние 3 года, основные векторы проникновения в корпоративные и ведомственные сети, среднее время нахождения злоумышленника в инфраструктуре жертвы и т.п. Это хоть и не было ново — ровно те же тенденции озвучиваются и многими другими компаниями, но



показало, что те данные, которые все субъекты КИИ, а также иные субъекты ГосСОПКА направляют в неё, не пропадают даром, а используются для подготовки бюллетеней, рассылаемых по закрытым спискам получателей, а также для выработки рекомендаций по отражению атак и применению современных технологий ИБ.

Однако надо признать, что этот SOC-Форум мог стать последним, на котором представители НКЦКИ так подробно рассказывали о своей деятельности. Вспоминая пресловутый приказ ФСБ «Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранным государством, его государственными органами, международной или иностранной организацией, иностранными гражданами или лицами без гражданства могут быть использованы против безопасности Российской Федерации», данные о ГосСОПКА и инцидентах на объектах оборонно-промышленного комплекса относятся к достаточно странной категории данных, которые, с одной стороны, и не отнесены прямо к гостайне, а с другой — их раскрытие может повлечь за собой обвинение по статье «государственная измена». Учитывая, что и Минобороны, и Росгвардия, а также иные органы правопорядка, обороны и безопасности разработали схожие перечни, можно признать, что практика засекречивания чувствительной информации, которая относится к безопасности, будет только усиливаться.

SOC И ГОСОРГАНЫ

С другой стороны, ГосСОПКА подтолкнула многие государственные органы к тому, чтобы создавать у себя ведомственные центры мониторинга и реагирования на инциденты, и на прошедшем SOC-Форуме очень много выступлений было посвящено именно тому, как различные ведомства выстраивают работу по обнаружению угроз и с какими сложностями они сталкиваются. Например, ДИТ Москвы рассказывал о своём созданном ведомственном центре, который в меньшей степени является классическим SOC, делегируя эту функцию органам исполнительной власти и учреждениям Правительства Москвы. При этом ДИТ Москвы координирует все эти ведомственные SOC, собирает данные об инцидентах от них, проводит их анализ, а также занимается повышением уровня осведомлённости. А вот Минэкономразвития пошёл по другому пути. У них, в отличие от ДИТа и Минздрава, гораздо меньше подопечных и подведомственных организаций, поэтому они вполне могли себе позволить не строить собственный центр компетенций, а отдать его на аутсорсинг. Что они в итоге и сделали.

А вот Свердловская область пошла по гибриднему варианту — строит собственный SOC и пользуется услугами аутсорсингового коммерческого центра. При этом, судя по общению на форуме, многие сталкиваются с «сыростью» отечественных программно-аппаратных решений, которые применяются (или вынуждены применяться, если мы

говорим о госорганах) в центрах мониторинга в соответствии с требованиями правительства и регуляторов. Помимо технологий, проблемой являются и кадры, что приводит многие SOC к идее аутсорсингового SOC, который для многих госорганов, не имеющих людей и денег на их наём, является выходом из сложившейся ситуации. Однако, судя по выступлениям и разговорам в кулуарах, у госорганов выбор между аутсорсинговыми центрами мониторинга не очень богатый — по сути, выбирают из 2–3 игроков. Если же говорить о собственном центре предотвращения киберугроз, то почти все государственные SOC упоминали, что их штатная численность насчитывает 10 человек. Думаю, можно использовать эту цифру как некий эталон для SOC начального уровня.

Наиболее глубоко (по сравнению с другими госорганами) тема SOC была раскрыта для здравоохранения, так как Минздрав в преддверии SOC-Форума создал отраслевой центр ИБ (отраслевой сегмент ГосСОПКА), о работе которого и рассказывалось для организаций здравоохранения на закрытой секции.

SOC И ТЕХНОЛОГИИ

С технологической точки зрения, как ни странно, ничего нового на форуме не прозвучало. Возможно, это было связано с тем, что основные выступающие представляли всё-таки аутсорсинговые центры мониторинга, которые не хотели делиться с конкурентами своими секретами. Возможно, причина в том, что,



несмотря на курс на импортозапрещение, принятый в государстве, многие SOC по-прежнему базируют свой технологический стек на зарубежных решениях и не хотят привлекать внимания к этому (спонсорских выступлений про различные продукты было немало). А может быть, и секретов особых нет, а просто делиться нечем? В любом случае эта сторона центров мониторинга осталась почти не раскрытой, чего не скажешь о зарубежных мероприятиях, которые практически в те же дни проходили в Соединённых Штатах Америки.

На SOC Reload 2021 и Security Operations Summit как раз много говорили о различных технологических новациях, которые упрощают и обнаружение инцидентов, и их расследование, и реагирование на них. Тут и автоматизация работы с плейбуками, вплоть до применения low code/no code технологий, и автоматический сбор и классификация данных threat intelligence (и это не только фиды и IOC), и автоматизация работы с MITRE ATT&CK, и создание универсального каталога контента обнаружения, который может быть легко переносим между различными решениями по мониторингу, и даже про концепцию Detection-as-Code, которая сегодня тоже становится не просто модной, а жизненно важной. Но обо всём этом на SOC-Форуме не говорилось, что оставляет надежду на то, что следующие форумы будут больше внимания уделять этой теме.

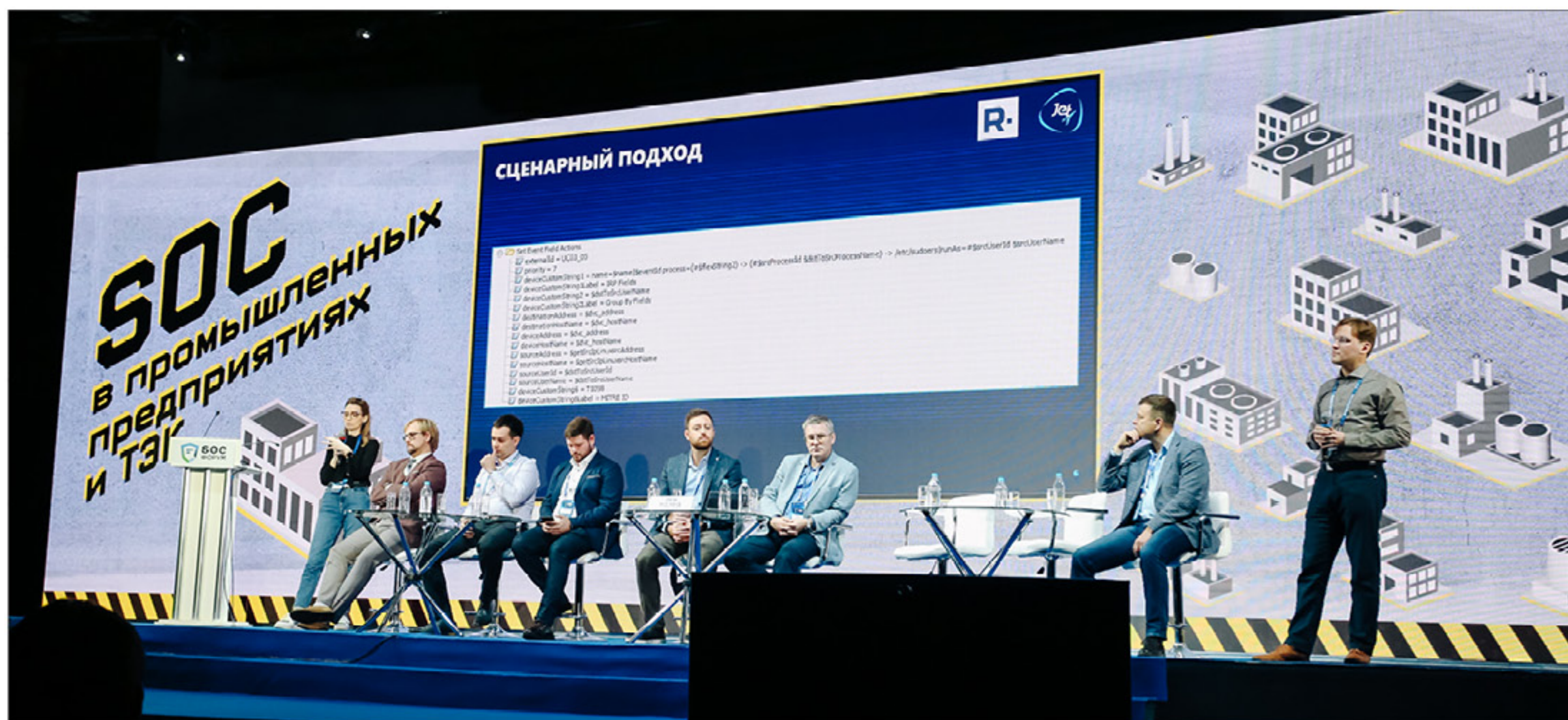
SOC И ЭКОНОМИКА

А вот то, о чём мало говорят на Западе, но пытались обсуждать на SOC-Форуме, — это вопросы экономики мониторинга и реагирования. Это очень важная тема, о чём нам говорит и один из классических тезисов ИБ — «безопасность не должна быть дороже защищаемой информации». Но как посчитать стоимость защищаемой информации? Увы, ответа на этот вопрос так и не прозвучало (тому, кто ответит на него, можно Нобелевскую премию вручить), но было несколько докладов, которые касались расчёта экономических показателей деятельности SOC с разных сторон — то с точки зрения цены инцидента (была названа цифра в 0,5 миллиона рублей для базовой атаки с применением шифровальщика), то с точки зрения затрат на создание собственного SOC. Правда, вновь пришлось столкнуться с некоторым лукавством, так как приведённые цифры были представлены поставщиками услуг аутсорсинговых SOC и они, что неудивительно, своими цифрами пытались доказать, что аутсорсинг функции мониторинга и реагирования — лучшая модель решения данной задачи.

Обычно авторы таких выступлений умалчивают об обратной стороне медали, а именно об эффективности аутсорсинговых SOC. Мне доводилось дважды модерировать на SOC-Форуме одноимённую секцию, и могу сказать,

что оба раза мало кто смог поделиться своим реальным опытом оценки эффективности мониторинга и реагирования и путями улучшения этих показателей. SOC-Форум 2021 не стал исключением: мало кто говорил об эффективности своих процессов. Ну разве что приводились маркетинговые цифры про количество инцидентов и скорость взятия инцидента в обработку (а это далеко не то, что интересно и нужно знать).

Например, выпущенное в дни проведения форума исследование Cisco Security Outcomes Study Vol.2 с цифрами в руках показало, что аутсорсинговые SOC реагируют на инциденты вдвое дольше, чем on-prem SOC, и хуже, чем гибридные SOC. Так что выбор между моделью функционирования SOC не так прост, как об этом говорят представители аутсорсинговых центров мониторинга ИБ и как это регулярно звучало на SOC-Форуме 2021. Выбор операционной модели SOC (on-prem, аутсорсинг, распределённая или вообще без SOC) — это важнейший вопрос при проектировании SOC, и если на него не ответить с самого начала честно, то потом SOC может развиваться по неверному пути, как и затраты на него. Я не зря про это писал в BIS Journal в преддверии SOC-Форума. Попытка создать целиком собственный SOC может обойтись дорого, а, например, гибридная модель SOC (что-то у себя, что-то у аутсорсера) даёт более



низкую эффективность обнаружения и реагирования, чем либо «всё у себя», либо «всё на аутсорс». Но справедливости ради надо признать, что в России пока просто нет адекватных данных, чтобы с цифрами в руках говорить об эффективности той или иной модели. Приходится критически оценивать чужие цифры.

SOC И АСУ ТП

Ещё одной особенностью SOC-Форума 2021 стало обсуждение темы мониторинга киберугроз на промышленных площадках. Но, несмотря на две большие сессии, посвящённые этому вопросу, каких-то ноу-хау или даже серьёзного практического опыта представлено не было. Всё-таки надо признать, что если тема SOC у нас развивается всего лет пять, то о безопасности АСУ ТП активно стали говорить чуть позже, а массовых проектов в этом направлении в связи с консервативностью отрасли пока не наблюдается. Жизненный цикл средств промышленной автоматизации, другие ответственные (не ИТ, а АСУ ТП), отличные от корпоративных сетей подходы к созданию промышленных площадок, иные приоритеты (доступность вместо конфиденциальности), отсутствие серьёзной мотивации... Всё это делает задачу ИБ в АСУ ТП более неповоротливой, чем в обычных офисных сегментах. И то же самое касается мониторинга промышленных

сетей, вмешательство в работу которых (даже в пассивном режиме) до сих пор остаётся камнем преткновения в среде специалистов.

Поэтому на SOC-Форуме были озвучены несколько основных сценариев мониторинга:

- ◆ выгрузка телеметрии об инцидентах на USB и загрузка их на централизованную платформу SOC.
- ◆ развёртывание локального изолированного мини-SOC.
- ◆ использование однонаправленных МСЭ для передачи телеметрии об атаках в централизованный корпоративный SOC.
- ◆ применение сценария C-Bridge.

Но узнать о практическом опыте их использования так и не удалось.

ЗАКЛЮЧЕНИЕ

Очень сложно в одной статье рассказать о том, что рассказывалось в течение двух дней на четырёх потоках SOC-Форума. Например, очень интересны были секции, на которых рассматривались различные практические сценарии работы SOC. Правда, их было не так уж и много (на фоне общего числа докладов), и их сложно пересказывать без погружения в детали. Например, интересным был рассказ об опыте мониторинга облачных инфраструктур (на примере MS Azure) или о передаче контента обнаружения при смене SOC или SIEM.

Не хотелось бы завершать обзор на негативной ноте, поэтому я опущу кадровый вопрос, который является больной темой в ИБ в последние годы и на SOC-Форуме в частности. К сожалению, на мой взгляд, эта задача не имеет быстрого решения, и сегодня многие игроки рынка часто используют не всегда корректные методы, просто перекупая специалистов у конкурентов и заказчиков, раскручивая тем самым гонку зарплат, что в итоге негативно скажется на всём рынке. Гораздо более позитивно выглядит тема эмоционального истощения (выгорания) сотрудников SOC, что, по итогам опроса 4,4 тысячи сотрудников 500+ работодателей в 2021 году, является общей проблемой для всех без исключения. Более 60% опрошенных либо испытали выгорание сами, либо находятся в этой стадии сейчас; оставшиеся наблюдали это явление у коллег (видимо, не хотят признаваться). А поскольку это явление носит массовый характер, способы борьбы с ним известны и могут быть относительно легко внедрены в работу SOC.

В целом прошедший SOC-Форум оправдал мои ожидания, показав, что тема мониторинга ИБ и реагирования на инциденты не просто живёт, но и развивается, пусть и не совсем так, как это происходит за рубежом.

FINOPOLIS 2021

О ТЕХНОЛОГИЯХ, КОТОРЫЕ «ПЛЕТУТ СЕТЬ ВОКРУГ НАС»

«МЫ БАНКИРЫ, МЫ ТАК ВИДИМ»

Конференция Finopolis 2021 и в камерном онлайн-формате оказалась весьма интересной. В ходе стартовой пленарной дискуссии «На кончиках пальцев: опыт взаимодействия человека с технологиями» откровенно, а в некоторых случаях откровенно критически комментировались перспективы модных «клиентоцентричных» стратегий — от суперсервисов до метавселенных. Занимались этим первые лица лидеров финансового рынка, а также самая богатая женщина России Татьяна Бакальчук и женщина, наиболее осведомлённая в предметной области конференции, — Эльвира Набиуллина.

Глава Центробанка выступила одновременно и адвокатом дьявола цифрового финтех, и его прокурором. Эльвира Сахипзадовна дипломатично расставила вешки сомнений в ряде мест «райского сада», которым представляется обществу цифровая экономика. Технологии финтех она сравнила с сетью, опутавшей каждого человека. Посулы «клиентоцентричности» сервисов были спроецированы ею на цену, которую придётся заплатить за подобную кастомизацию. Не обошла стороной Эльвира Сахипзадовна и ключевой вопрос той ESG-экономики, в которую мир вроде бы готовится войти: «...и точно ли это то, что нам нужно? Сможем ли мы в этой ситуации изобилия предложений сохранить здоровые отношения?»

Участники пленарки — Герман Греф, Пётр Авен, Андрей Костин и молодой банкир Татьяна Бакальчук — оказались приверженцами применения современных цифровых технологий. Упомянули как неизбежность широкое использование так называемого искусственного интеллекта, выступили в поддержку масштабного «бесшовного» и «прозрачного» перетекания персональных данных (ПД) между информационными системами государства и бизнеса — для реализации «социального скоринга», изложили каждый своё уникальное видение перспектив превращения бизнеса

в «клиентоцентричный» на основе суперприложений и экосистем... И единодушно, хотя и в разных выражениях, оценили идею метавселенной как преждевременную.

ОБЪЯТЬ НЕОБЪЯТНОЕ ИЛИ НУ ЕГО?

Приверженность руководства Сбера идеологии централизованной экосистемы хорошо известна. Для её воплощения банк покупает небольшие компании, имеющие сервисы, предположительно привлекательные для клиентов. Хотя Герман Греф и отметил, что приобретения эти не такие уж и затратные, как утверждают злые языки.

Андрей Костин, добродушно покритиковав идею экосистемы в видении Сбера и сравнив её с благоустроенным гетто, выступил сторонником менее затратного и более гибкого партнёрства.

А Пётр Авен оказался консерватором, считая, что разбрасываться по разным направлениям банку не пристало. Для успешности бизнеса следует хорошо делать своё — банковское — дело, предоставив клиенту возможность свободно искать дополнительные сервисы «на стороне». Хотя и идею партнёрства он не отвергал, оставляя при этом за клиентом большую свободу выбора, нежели та, что реализуется в экосистемном «гетто» или партнёрстве «по ВТБ».

Также Пётр Авен обратил внимание на возможный негативный эффект для банковского бизнеса в виде потери лояльности со стороны клиента в случае некорректной работы хотя бы одного сервиса экосистемы.

НЕМНОГО ДЁГТЯ

Критическим оказался и настрой в отношении социальных последствий цифровизации. В частности, был покритикован тезис об экономии времени человеком, который «в один клик может получить то, что хочет».

Вот, например, комментарий главы ВТБ: «Цифровизация привела не к экономии, а к огромной трате времени. Откройте родительский чат,

обсуждающий, что подарить детям к Новому году, и поймёте, что даже если родители договорятся, то потратят на это в два-три раза больше времени, чем если просто поедут в магазин и купят какой-то подарок. Обсуждение всего в Интернете, начиная с одежды известной теледивы и заканчивая вопросами школы, поглощает уникальное количество времени!»

В числе отрицательных сторон цифровизации была упомянута и растущая потребность населения в «пустом» общении в соцсетях или мессенджерах.

По мнению Германа Грефа, такого рода проблемы следует не просто видеть и критиковать, но искать пути их решения, разрабатывая и предлагая человеку варианты реального саморазвития за счёт высвобождаемого «цифрой» времени.

Не переоценили участники первой пленарки и возможности современных ИТ. Глава Сбера рассказал о собственном негативном опыте использования технологий дополненной реальности, а Э. С. Набиуллина косвенно покритиковала «алгоритмы идиотизма» (не используя, впрочем, напрямую этот термин Стива Возняка) на примере работы с «умной» музыкальной колонкой.

«НА СЛУЖБУ НЕ НАПРАШИВАЙСЯ!»

После безусловной поддержки лидерами идеи «социального скоринга» тема следующей пленарки — «Бесшовные рельсы цифровизации: возможно ли это?» — выглядела развитием дискуссии о возможности положительного опыта взаимодействия человека с технологиями.

Казалось бы, такая дискуссия — самое место для обсуждения принципиальных проблем от самой по себе необходимости тотальной цифровизации страны до её допустимых масштабов с учётом реалий национальной технологической независимости и возможности обеспечить безопасность такой системы. По крайней мере, можно было бы обсудить распределение ролей между государством и бизнесом.

Но, похоже, КРІ под такого рода работу в Минцифры пока нет. Министерство в основном говорило о «допиливании» своего так нелюбимого согражданином «ИТ-ребёнка» в виде ЕБС. На сегодня к этой системе «прикручиваются» интерфейсы, призванные «упростить процесс сдачи биометрии» для того, «чтобы у пользователя возникла мотивация сдавать свою биометрию».

Тогда как ИМХО ключевая проблема для возникновения такой мотивации — обеспечение гарантий информационной и кибербезопасности (ИБ&КБ) комплекса ЕБС и предоставление гражданам убедительных доказательств наличия таких гарантий. Гарантий технологических и правовых.

Вместо этого был разрекламирован запуск процесса получения ЕСИМов — электронных SIM-карт без физического носителя — с помощью ЕБС. И это на фоне тлеющих скандалов с махинациями вокруг использования электронных «подписей» и мошеннических «корпоративных SIM-карт» (пока на классических физических носителях). А уж если у мошенников появится ещё и возможность получать ЕСИМы, «сдав биометрию не приходя ни в МФЦ, ни в банк»...

Уместно заметить, что на второй дискуссии всё же говорилось о проблемах ИБ&КБ. Но не со стороны государства, а из уст консерваторов Альфа-Банка (на этой дискуссии уже в лице его главного управляющего директора В. Верхошинского), и были произнесены лишь самые общие слова о желательной необходимости создания некоей платформы для отработки навыков и приёмов. Минцифры не проявило желания поучаствовать в обсуждении озвученной проблемы. ФСТЭК, ФСБ и соответствующие структуры Банка России на обсуждении вообще не присутствовали.

ОХ УЖ ЭТИ ПД!

Из дискуссий стало понятно, что правоприменение и правопослушание в отношении законодательства об обороте ПД у нас вполне обычное: «Строгость российских законов смягчается необязательностью их исполнения». При этом участники обратили внимание, что наши граждане сами по себе склонны к проявлению в соцсетях

«душевного стриптиза», что снимает с финансово-кредитных организаций бремя этических страданий при сборе и использовании ПД.

Если же, минуя мораль, руководствоваться только буквой закона, то, по словам представителя Роскомнадзора на секции по вопросам оборота ПД, когда есть сомнения в принадлежности или непринадлежности информации к ПД, то её нужно считать ПД.

Более приемлемой «на земле» выглядела всё же позиция лидеров финансового рынка, тем более что при необходимости можно прикрыться рассуждениями о безопасности использования «обезличенных» ПД, об обеспечении должного уровня защиты прав номинальных «владельцев» ПД, обработкой данных только в интересах «достижения заявленных целей» и другими соображениями, вполне укладывающимися в такие реалии, как «закон что дышло...».

Ведь бизнес-аналитики и ИТ-визионеры уже ряд лет поддерживают мнение о перспективах работы с «цифровым профилем» клиента — в виде дополнительных доходов. А «ведущие ИТ-компании» готовы предоставить инструментарий для составления таких «цифровых профилей» и оказать услуги по эффективному его использованию.

Вот один из комментариев: «На рынке известны ситуации, когда и страховые компании, и банки обращаются к компаниям ИТ-сектора, чтобы сформировать более взвешенный подход к коммуникации с клиентом, анализируя историю поиска клиента, переписку и много других параметров, о которых современные граждане могут даже не догадываться».

Однако уместно заметить, что в ситуации, когда при проведении скоринга страховщиками анализируется от 40 до 80 параметров, а в практике банков количество параметров может исчисляться тысячами, под критерии оценки «добро на выдачу кредита» могут попасть и ненадёжные заёмщики. Что доказывается тревогой Центробанка в связи с ростом задолженностей по кредитам по всей стране.

И НЕМНОГО О ПРАКТИКЕ

«Цифровая ипотека» и приход на рынок розничного инвестора на волне

технологии «инвестирования в несколько кликов» (лёжа на диване) — это темы Finopolis 2021, призванные представить практику «бесшовности» и «одного окна». Их обсуждение состоялось, было сказано много обнадеживающих слов о текущей пользе и грядущих перспективах. В том числе и о достижении высот в сфере воспитания нового Человека, который уже якобы прошёл этапы «стремления к зарабатыванию денег» и «любви к трате денег».

Но, как оказалось, ещё даже не решён вопрос, где должно находиться то самое «одно окно», в котором «бесшовно» будет оформляться «цифровая ипотека». А розничного инвестора по итогам года ожидают, скорее всего, обескураживающие результаты. Хотя г-н Вьюгин, представлявший Московскую биржу, произнёс лестные слова в адрес этого самого инвестора, который, во-первых, пришёл-таки на рынок, а во-вторых, неприхотлив в своих ожиданиях.

НА ПОСОШОК

Есть основания предполагать, что обсуждение «возможностей применения цифровых технологий в финансовом секторе» неактуально в контексте оценок «возможности» или «невозможности». Как хороший двигатель позволяет летать и бревну, так и современные процессоры, ПО, языки программирования и системы коммуникаций позволяют многое.

«Возможности применения» практически безграничны, и тут не о чем спорить. Но раскрытие этих самых «возможностей применения» актуально только в контексте возможностей безопасного применения — как с точки зрения кибербезопасности задействованных ИТ-архитектур и систем, так и обеспечения технологической независимости при их использовании (ведь мы уже балансируем на грани, присядьте на стульчик, запрета поставок мобильных телефонов).

А также не стоит забывать, что раскрытие «возможностей применения» тесно связано с пониманием реальных потребностей Человека. И с пониманием того, «чем платит человек за это удобство, дешевизну, комфорт...».

Но это, как оказалось, никого не волнует. Кроме Э.С. Набиуллиной.

МОРАЛЬ КАК ПОСЛЕДНЕЕ ПРИБЕЖИЩЕ ИБ

КОНФЕРЕНЦИЯ БАНКА РОССИИ О ПРОМЕЖУТОЧНЫХ ИТОГАХ РАБОТЫ ЗАКОНА № 224-ФЗ

Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком...» нечасто упоминается на специализированных мероприятиях, посвящённых информационной безопасности. Хотя навскидку противодействие инсайду в финансовой сфере имеет прямое отношение к управлению конфиденциальностью информации. Да и для управления рынком удобно манипулировать целостностью и доступностью околофинансовой информации. Тем более когда подобные действия с недобросовестными намерениями можно благопристойно укрыть за ширмой мер якобы противодействия «неправомерному использованию инсайдерской информации».

ЧЕГО В ЭТОМ БОРЩЕ НЕ ХВАТАЕТ?

Тем не менее конференция Банка России «Противодействие инсайду и манипулированию рынком: в поисках новой парадигмы» не включила экспертов из сферы информационной безопасности в число своих панелей, а выступившие на конференции в силу неясных причин детально не обсуждали уместный опыт финтех и служб ИБ.

В те моменты, когда предпринимались отчаянные попытки найти парадигму противодействия недобросовестным практикам, явно не хватило присутствия экспертов по антифроду, которых в изобилии можно встретить на классических «ибэшных» мероприятиях

На конференции лишь «по скользкой» было упомянуто о таких явлениях, как автоматизированная («высокочастотная») торговля биржевыми активами, программные приложения, используемые для манипулирования рынком (и практика уголовного преследования за рубежом создателей такого ПО), «аналитическое и математическое исследование информации», которой «так много, что трудно определить, где она точная, а где сфабрикована».

Пренебрежение вызовами цифровизации тем более странно, что тема первой панельной дискуссии была сформулирована как «Итоги 10 лет закона об инсайте: большие надежды и вызовы новой реальности». Получается, что финтех и процессы «цифровой трансформации» не были отнесены организаторами конференции к значимым вызовам новой реальности. В отличие от, например, «поколения Reddit» — явления, название которого было вынесено в тему отдельного круглого стола о частных инвесторах на бирже.

Это обстоятельство заставляет в очередной раз задуматься о реальном месте финтеха и цифровой трансформации в иерархии ценностей здорового финансового рынка. Задуматься в противовес навязываемому стереотипу восприятия цифровизации как панацеи, как новой технической революции. Задуматься в противовес

манипуляциям с терминологией, когда автоматизация и автоматика упорно связываются с проявлениями интеллектуальной деятельности программно-аппаратных платформ для снятия ответственности с человека.

Что же касается самой конференции, то в качестве наиболее значимых инструментов для реализации регуляторных задумок закона № 224-ФЗ были названы: внедрение в «ДНК» рынка «гена» нетерпимости к недобросовестности и развитие культуры рынка в виде системы табу и ограничений на недобросовестное поведение.

КТО ВИНОВАТ?

Закону № 224-ФЗ не только минул первый десяток, но он так же, не менее 10 лет, вынашивался до своего принятия регулятором, встречая жёсткое противодействие с разных сторон, включая СМИ, вопиющие о цензуре (об этом напомнила руководитель Центра законодательных инициатив ВЭБ.РФ Т.М. Медведева).

При этом уместно заметить, что без этого закона рынок жил и рос до 2007 г., рухнул в 2008 г. и до сих пор не восстановился до уровня 2007 г., хотя с 2010 г. и живёт под сенью 224-ФЗ. Тем не менее регулятор и околорегуляторные службы возлагают на него большие надежды в контексте создания доверия к рынку. Наверное, поэтому все выступавшие на конференции старались говорить о законе или хорошо, или ничего.

А вот о текущем состоянии культуры рынка говорили плохо. Был упомянут, в частности, живучий стереотип «заработать на рынке можно лишь нечестным путём». А также широкая поддержка в нашем обществе лжи и воровства как новых норм поведения.

Эксперты отметили, что формальность определений и норм закона



Запись онлайн-трансляции конференции доступна на YouTube-канале Банка России: youtube.com/watch?v=cL48WULDeVs

№ 224-ФЗ усугубляется низким качеством правоприменения на территории России, что не позволяет в ряде спорных случаев «правильно трактовать закон». В результате «рынок пропитан инсайдом, и никто не боится им пользоваться».

Уместно заметить, что и в самом законе заложены корни зла: его положения, например, неприменимы к действиям органов власти всех уровней, притом что эти органы являются «сильной стороной» во всех жизненных обстоятельствах. Например, разгон инфляции этой «сильной стороной» является только одним из «вызовов новой реальности».

Если выделить подобные печальные факты на фоне рассуждений о возможных механизмах искоренения пороков, на борьбу с которыми мобилизован № 224-ФЗ, то оснований для оптимизма практически не остаётся. Хотя представление о справедливости, которая в головах людей нашей страны традиционно выше закона, требует, чтобы «инвестор не был объектом, на котором наживаются» (цитата конференции) и ему было гарантировано право на всеобъемлющую «прозрачность» информации.

ЧТО ДЕЛАТЬ?

Руководители инвестиционных и брокерских бизнесов, участвовавшие в конференции, явно не лучились

оптимизмом по части проявления на рынке «гена нетерпимости к недобросовестности». И в то же время панелисты и эксперты, представлявшие службы внутреннего контроля, аудита, комплаенса, взаимодействия с органами власти и общественными организациями, активно направляли конференцию в русло поиска механизмов для повышения доверия к рынку инвестиционных спекуляций.

Любопытно, что эксперты конференции не стали предлагать путь гармонизации отечественных практик с практиками североамериканского и европейского рынков. «Допустимые на американском рынке стратегии недопустимы в России» (цитата конференции). Вместо гармонизации чужого опыта регулятору было предложено сформировать перечень либо недобросовестных практик, либо добросовестных. В любом случае у игроков появится одобренное регулятором руководство к действию.

В качестве то ли шутки, то ли от безысходности ситуации с моралью на рынке было предложено учредить медаль для честных брокеров и проводить их отбор в профессию на основании в том числе и оценки законопослушности в быту (например, при оплате штрафов за неправильную парковку).

В общем, было много живого, интересного. И всё же на конференции,

особенно в те моменты, когда предпринимались отчаянные попытки найти парадигму противодействия недобросовестным практикам, явно не хватило присутствия экспертов по антифроду — именно тех, кого в изобилии можно встретить на классических «ибэшных» мероприятиях. Мне, например, вспомнился доклад компании ITD Group, прозвучавший на конференции AntiFraud Spring Russia 2021. Он напрямую был посвящён решениям для выявления высокоуровневых противоправных действий в ходе финансовых спекуляций банками и «проприетарных» финансовых операций банков на рынках акций.

В КАЧЕСТВЕ ВЫВОДА

Что стало понятно? Усилий по морально-нравственному усовершенствованию рынка недостаточно. Необходимо также и совершенствование регуляторики. Это касается и уточнения списка субъектов, способных манипулировать рынком (например, расширения сферы действия закона № 224-ФЗ на «внесистемных» аналитиков и экспертов, влияющих на рынок через каналы социальных сетей и иные медиаканалы), и расшивки коллизии нынешних представлений об инсайдерской информации, и права добросовестных инвесторов на «прозрачность» информации.

СYBERCRIMECON 2021. ЩЕЛИ АДА

О ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРЕСТУПНОГО МИРА

Конференция CyberCrimeCon проводится под эгидой компании Group-IB и является одним из немногих отечественных мероприятий, посвящённых непосредственно киберкриминалистике. В этой сфере вопросы права тесно переплетены с технологическими новациями и часто трудно понять, где «тёмная» сторона, а где «светлая». Например, киберпреступники часто используют в своих целях цифровую инфраструктуру «белой» экономики, в частности популярные онлайн-сервисы, и широкодоступные решения финтеха — фейковые платёжные системы часто с блеском используют автоматизацию для мошеннических транзакций.

Как ни прискорбно, но ИТ-инновации открывают новые горизонты для неправомерных действий, выводя криминальные, по сути, деяния из-под козырька возможностей правовых органов. С другой стороны, расследование «высокотехнологичных» преступлений невозможно без соответствующих знаний и опыта, что сегодня также является дефицитом.

ПО ПОВЕСТКЕ

В нынешнем году на CyberCrimeCon докладывались результаты расследования деятельности группы EvilCorp, на которую был повешен ярлык «самой опасной»; примеры использования инструментария Cobalt Strike для

атак на «европейские правительства»; обсуждалась деятельность «ранее неизвестной шпионской АРТ-группы», которая считается ответственной за атаки на энергетический, авиационный и государственный секторы экономик разных стран и многое другое.

Помимо специалистов из Group-IB, своё видение текущей ситуации и тенденций в развитии киберпреступности представили эксперты Интерпола и Европола, и в том или ином объёме были затронуты болевые точки кибербезопасности практически по всему миру (Европа, Соединённые Штаты Америки и Канада, Африка, Азиатско-Тихоокеанский регион) и в разных сферах (энергетика, авиационная и другие отрасли, государственный сектор).

Предметом гордости Group-IB стало её успешное участие в операции Carding Action под эгидой Европола, позволившее европейским финансовым учреждениям предотвратить потенциальные убытки на сумму около €40 млн. При этом Group-IB является, как утверждают некоторые СМИ, официальным партнёром не только Европола, но и Интерпола.

Также были представлены доклады, на которых обсуждались уязвимости, казалось бы, обкатанной технологии Java и уязвимости платформы Zoom, обретшей популярность благодаря массовой антиковидной удалёнке, но фактически только-только проходящей «бевую» апробацию.

НЕКОТОРЫЕ ВЫВОДЫ

На конференции отмечалось, что сегодня киберпреступность использует не только современные достижения ИТ-инженерии, но и эффективные деловые подходы к организации своей деятельности. В качестве примера сложного разделения труда приводилось сотрудничество двух групп хакеров — работающих с программами-шифровальщиками и тех, кто специализируется на взломах корпоративных сетей и продаже информации об их уязвимостях.

Подобная специализация, как и в «белой» экономике, позволяет обеспечить высокую производительность «труда» и, соответственно, более высокий доход для всех участников «производственной цепочки».

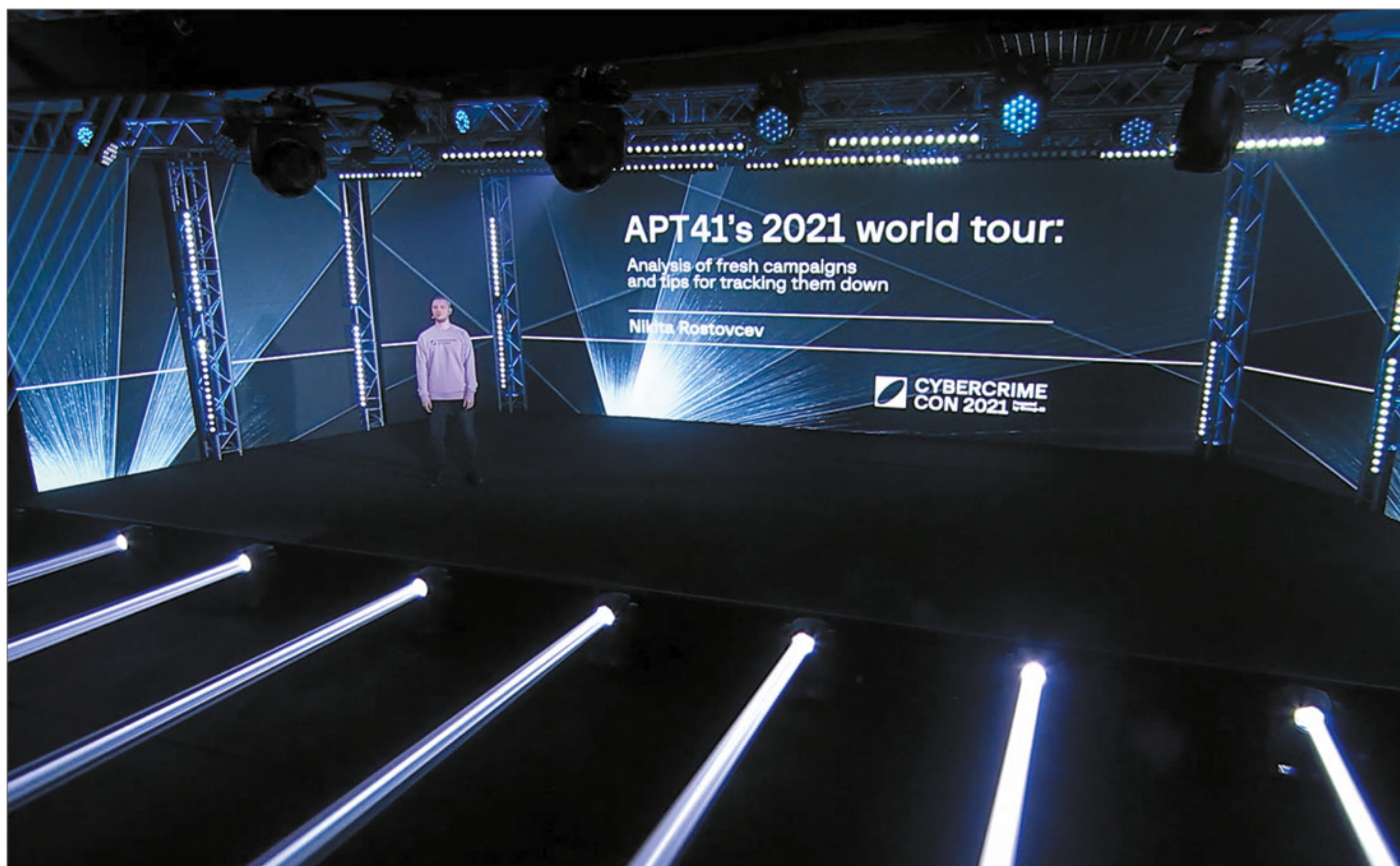
Интересно отметить, что одновременно меняется и уточняется терминология. Грубый «зонтичный» термин «хакер» ныне замещается благозвучными «оператор программ-вымогателей», «брокер начального доступа» (это про тех, кто взламывает корпоративные сети) и другими «цивильными» выражениями. Складывается впечатление, что скоро появятся и соответствующие профстандарты.

Подобные факты и сопровождающие их цифры о теневых доходах киберсообщества указывают на то, что киберпреступность превращается в своеобразную отрасль экономики, стимулирующую, как это ни парадоксально, научно-технический прогресс и открывающую новые возможности для социальных лифтов в обществе.

СТАРЫЕ КОЛЛИЗИИ В НОВОМ ИНТЕРЬЕРЕ

В связи со сказанным на ум приходит историческая аналогия, когда английские пираты получали «госаккредитацию» для проведения разбойных операций, а позже самые успешные душегубы пополняли ряды английской элиты.

Грубый «зонтичный» термин «хакер» ныне замещается благозвучными «оператор программ-вымогателей», «брокер начального доступа» (это про тех, кто взламывает корпоративные сети) и другими цивильными выражениями



А если вспомнить о широко известных фактах сотрудничества американских госорганизаций и общественных объединений с мафиозными структурами, то легко понять, что цифровизация открывает новые возможности для управления внутри- и межгосударственными отношениями. И не только на уровне государственных органов, но и со стороны так называемых глубинных правительств.

И тут необходимо обращать внимание не только на «общезакономерные» и политические угрозы. В таком контексте тотальную цифровизацию можно сравнить с «щелями ада», выпускающими на поверхность демонов всех мастей.

Возникают (и уже проявляются) угрозы ИТ-сообществу (и компаниям, и конкретным персонам), которое оказывается втянутым (нередко втёмную) в межгосударственные разборки и конфликты игроков глобального бизнеса и глобальной политики. Тем более что одна из граней этих «тёрок» — возможность нанести противнику репутационные потери, перевести стрелки общественного возмущения на

непричастных и невиновных. Например, создать и культивировать в мире бренд «Русский хакер», выращенный из реликтовых страшилок о «русском медведе с ядерными ракетами».

В связи с этим вполне естественным шагом является проведение мероприятий, подобных CyberCrimeCon, в формате информационных витрин, но не для всех инициатив и возможностей. Важную роль в оформлении таких «витрин» должна играть корпоративная цензура (её наличие в современном бизнесе трудно отрицать), которая не позволит развешивать персональные, национальные и иные ярлыки там, где уместны лишь инженерные и методологические оценки.

О НАЦИОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ

Одной из современных реалий является аморфизация понятия «национальная компания». Это связано с глобализацией в сфере технологий, подбора персонала, размещения офисов и штаб-квартир компаний. Это явление совершенно очевидно наблюдается в мире отечественных ИТ-компаний.

Оно сопровождается коллизиями в налоговой сфере, но к ещё более острым противоречиям размытие национальной идентичности может привести, когда затронет компании, способные играть важную роль в создании оборонного киберщита.

На фоне сказанного вызывает тревогу утверждение организаторов CyberCrimeCon о том, что площадка конференции создана для «обмена последними находками, исследованиями и обновлённой экспертизой» и предоставляет «уникальную возможность получить ценные инсайты и данные».

Очень бы хотелось усомниться в искренности такого утверждения. Ведь подобная информация — это скорее предмет закрытых встреч и совещаний, проходящих под грифами «для служебного пользования» и выше, с учётом той роли, которая отводится киберпространству в нынешних межгосударственных политических и экономических противостояниях.



Валерий КУЛИКОВ
обозреватель BIS Journal

OS DAY 2021, ROSS 2021

ПУТЬ СПО. ЛОКОМОТИВ OPEN SOURCE ВСТАЛ НА ПРАВИЛЬНЫЕ РЕЛЬСЫ?

Последний квартал прошлого 2021 года ознаменовался конструктивным оживлением в тех сферах отечественных ИТ, что намерены заняться покорением высот импортозамещения, используя продукты и технологии, предоставляемые «МетаВселенной» Open Source.

Своеобразным анонсом нового этапа работ по обретению ИТ-независимости стали выступления замдиректора ФСТЭК России Виталия Лютикова и гендиректора АНО «Цифровая экономика» на BIS Summit 2021. Было заявлено, что Open Source должен стать локомотивом разработок в отечественной ИТ-отрасли, однако локомотив этот надо переставить на отечественную колею (помня о санкциях и импортозамещении) в части поддержки процессов разработки и верификации/сертификации.

И менее чем через месяц после этого в рамках конференции OS DAY 2021 был проведён круглый стол «Безопасность ядра: единство и разнообразие» — своеобразное оргсобрание участников работ в Технологическом центре исследования безопасности ядра Linux (далее — ЦЕНТР), создаваемого под эгидой ФСТЭК России.

ТАК ГОВОРИТ ФСТЭК

По замыслу ФСТЭК стратегическая цель ЦЕНТРА — создание методологии исследования безопасности ядер операционных систем (в принципе любых, как создаваемых на основе Open Source, так и проприетарных) и

создание обоснованной и апробированной на практике системы сертификации безопасности ядер ОС.

При этом поэтапно будут решаться несколько тактических задач. Среди них — организация более тесного взаимодействия игроков рынка и устранение технологического параллелизма в их работе, повышение уровня компетентности компаний, ускорение работ по устранению уязвимостей выведенных на рынок дистрибутивов ОС.

В числе проблем, которые предстоит преодолеть, были названы:

- ♦ сильная зависимость от иностранного сообщества (организационная и интеллектуальная);
- ♦ критический недостаток ресурсов (небольшой размер отдельных отечественных компаний и общий кадровый «голод»);
- ♦ технологическая «какофония» (использование широкого спектра версий ядра Linux, включая тупиковые ветки).

ДИАЛЕКТИКА ОСОЗНАНИЯ «ТЕХНОЛОГИИ» OPEN SOURCE

Упомянутому круглому столу предшествовал Russia Open Source Summit (ROSS 2021), официальным поводом для проведения которого стало обсуждение проекта документа «Стратегия развития программного обеспечения с открытым кодом в России до 2024 года». Этот материал, помимо прочего, официально разрушил все ранее возникшие заблуждения относительно того явления, что переводится и как «открытое ПО», и как «свободное ПО» (СПО).

При этом «Стратегия...» содержит указания на те области, направления и программы научно-технологического развития России (таковых несколько десятков), где следует учитывать её положения. В первых строках среди прочих — «Стратегия национальной безопасности Российской Федерации» и «Доктрина информационной безопасности Российской Федерации», утверждённые Указами Президента РФ.

На протяжении нескольких последних лет представители ФСТЭК России неоднократно обращали внимание на необходимость слома ситуации с пассивным восприятием тотальной технологической зависимости российских ИТ от проприетарного зарубежного системного ПО и проприетарных средств разработки приложений и, как следствие, зависимости отечественных разработчиков прикладного софта от проблем зарубежных вендоров и проблем с зарубежными вендорами.

Однако до сих пор в нашей стране так и не были сформированы авторитетные и работоспособные органы для ответственного планирования мер по преодолению упомянутой технологической зависимости и для ответственной реализации этих планов. Зато есть такой негативный опыт, как невыполненный план перехода учреждений государственной власти и федеральных бюджетных учреждений на СПО.

План был принят в Российской Федерации в конце 2010 года и не был выполнен. Не менее печально, что не были извлечены уроки из этого срыва.

И можно лишь предположить, что технологической первопричиной неудачи стали ложные стереотипы восприятия Open Source («мифы СПО»), разрушение которых «Стратегией...» было столь одно-моментно всеохватно, что, похоже, ещё и сегодня не до конца уложилось в головах людей, выросших и продвинувшихся по «карьерной лестнице», в том числе и благодаря ссылкам в разное время на ныне развенчанные «мифы СПО», собираемые в прошлом этими людьми в наиболее выигрышные по ситуации комбинации. И уместно заметить, что хотя бы один из мифов да и проскальзывал время от времени в статусе «true» при переводе мыслей некоторых спикеров и участников ROSS 2021 в формат речи.

НЕКОТОРЫЕ ИТОГИ КРУГЛОГО СТОЛА «БЕЗОПАСНОСТЬ ЯДРА: ЕДИНСТВО И РАЗНООБРАЗИЕ»

Зато такого рода оговорки не встречались в выступлениях участников Круглого стола «Безопасность ядра:

единство и разнообразие», проведённого 14 октября 2021 года в рамках конференции OS DAY 2021. В ходе обсуждения его участники, имеющие опыт нескольких десятков лет практических экзерсисов с СПО, «накидали» довольно много пожеланий к точкам пристального внимания ЦЕНТРА и направлениям его деятельности.

Было обращено внимание, в частности, на особенности, предъявляемые СЗИ-оборудованием к ядру ОС (по сравнению с требованиями вычислительной техники «общего назначения»); на необходимость увязки решения проблем безопасности ядра ОС с решением проблем безопасности библиотек; на то, что безопасная разработка тесно связана с наличием и безопасностью инструментария разработчика, который, в числе прочего, должен быть заточен под отечественные аппаратные платформы. И что называется, до кучи из зала пришли дополнения о возможностях и необходимости бороться с уязвимостями ядра не

только закрытием дыр, но и с помощью архитектурных методов.

Подводя итоги обсуждения, заместитель руководителя ФСТЭК России Виталий Лютиков:

- ♦ очертил реалистично выполнимый круг задач, которые следует решить Центру в ближайшие несколько лет («Широко шагая, можно порвать штаны!»);

- ♦ поручил создать работоспособную экспертную группу для «образмеривания» работ Центра;

- ♦ поручил подготовить инфраструктуру для совместной работы специалистов в рамках деятельности Центра.

АЭРИРОВАНИЕ ТИХОГО ОМУТА РАН

Проведение упомянутого круглого стола на OS DAY 2021 свидетельствует о начале реальных шагов по вовлечению в согласованную работу ШИРОКОГО круга ИТ-компаний, тех, что уже давно индивидуально «пасутся» на «делянке» Open Source, но чьи разрозненные знания не складываются в общую картину.

МИФЫ СПО

1) Мнимая бесплатность.

В реальности отсутствие лицензионных отчислений не означает бесплатности, а расходы на техническую поддержку, затраты на адаптацию и эксплуатацию ПО, переобучение персонала могут оказаться сравнимыми со стоимостью лицензии проприетарного аналога.

2) Мнимая «ничейность».

В действительности у открытого ПО есть авторы и правообладатели, права которых определены в лицензиях и защищены соответствующими законами. Их нарушение так же не оправдываемо и наказуемо, как нарушение лицензий на проприетарное ПО.

3) Мнимая бóльшая безопасность.

Открытость кода облегчает поиск уязвимостей как для защищающейся, так и для атакующей стороны. При большом объёме и сложности кода поиск уязвимостей очень затруднён и существует возможность злонамеренного внесения уязвимостей в продукт.

4) Мнимая гибкость.

Возможность комбинировать различные открытые компоненты для получения комплексных решений существует, но требует высокой компетенции ИТ-специалистов и зачастую повторения ими работы друг друга вместо приобретения готовой системы у производителя/поставщика.

5) Мнимая бóльшая надёжность.

Надёжность ПО не зависит от его открытости. Использование открытого кода требует технической поддержки не в меньшей степени, чем для проприетарных продуктов. Поскольку техническая поддержка подразумевает оперативное исправление ошибок, она требует компетенций разработчика данного продукта. Самостоятельная поддержка ПО пользователями в общем случае невозможна, а поддержка сообществ лишена каких-либо обязательств.

Возможно, для восстановления здравого смысла в ИТ-образовании имеет смысл создать образовательный аналог ФСТЭК и ему поручить, например, возродить культуру получения знаний в системе отечественного образования

А вот с вовлечением в совместную работу:

- ♦ разработчиков ОС «общего назначения» на основе ядра Linux — компаний ГК Astra Linux, «Базальт СПО», Открытая мобильная платформа, «РЕД СОФТ»;

- ♦ разработчиков СЗИ на основе ядра Linux (на круглом столе были «Код безопасности», «ИНФОТЕКС», «БеллСофт», представитель которого пообещал в ближайшем будущем интересные анонсы);

- ♦ разработчиков аппаратных решений (в числе приглашённых на мероприятия оказались МЦСТ, АО НПЦ «ЭЛВИС»);

- ♦ а также отечественных системообразующих сервисных ИТ-гигантов, которые были представлены на круглом столе «Яндексом»;

— возможно решение тех задач и достижение тех целей, которые сформулированы ФСТЭК России.

Уместно заметить, что ряд наблюдений и комментариев на круглом столе и изучение материалов СМИ указывает на то, что и до 14 октября 2021 года уже существовал некий Центр, имеющий отношение и к теме Linux, и к ИСП РАН.

Однако решить задачи, поставленные ФСТЭК, только с помощью Академии наук в нынешнем состоянии РАН невозможно.

Во-первых, потому что нынешние ИТ-научные сотрудники, изначально «заточенные» своими профессиональными деформациями на схоластику исследования «сферических коней в вакууме», не демонстрируют способностей и готовности «соскочить с подножки» идеологии непрерывных изменений в СПО и прочно обосноваться в парадигме «стабильной платформы». А без стабильной платформы невозможно говорить об управлении

безопасностью критичных процессов «по требованиям».

Во-вторых, даже принятие парадигмы «стабильной платформы» само по себе не обеспечит быстрой перестройки исследовательских технологий из-за банального отсутствия у перспективного академического контингента ИСП РАН («Сегодня в Институте сложился хороший костяк — 75–80% сотрудников моложе 40 лет») опыта ведения проектов в отечественных «полях».

Такой опыт есть у приглашённого «бизнеса», вкладом которого в активы ЦЕНТРА могут стать в том числе «приоритетные конфигурации», «опыт использования тестовых наборов», «сценарии работы с парольной и другой чувствительной информацией» и т.п., а также участие специалистов компаний в состоянии «стабилизации и расширения» (все заковыченные фразы и словосочетания взяты из доклада руководителя ЦЕНТРА).

ОТ КУЛЬТУРЫ НАВЫКОВ К КУЛЬТУРЕ ЗНАНИЙ

В основе таких «мифов СПО», как бесплатность и бóльшая надёжность, — игнорирование того обстоятельства, что «кадры решают всё». Этот вопрос в фоновом режиме был упомянут и на круглом столе 14 октября, а среди положительных итогов Russia Open Source Summit 2021 уместно отметить отпор сомнительной попытке поиска в методологии Open Source поддержки новомодного представления о так называемой свободной траектории образования (ответственность за выбор которой предлагается возложить на студента), отпор попытке проставления знака равенства между идеей «свободной траектории образования» и «системой Физтеха».

Коротко и со знанием ситуации была дана оценка идее «свободной

траектории образования» профессором ИТМО Анатолием Шалыто («студент, дай бог, лишь к концу вузовского обучения начинает осознанно подходить к выбору своего места в профессии»). При подведении итогов заседания секции «Развитие культуры Open Source разработки в университетах» представитель ИТМО не обошёл стороной и попытки искажения сути «системы Физтеха». Рождённый в годы, когда «физика стала родом войск», этот вуз как никакой другой знал, по какой именно образовательной траектории должны идти его питомцы, и добивался этого, загружая студентов по полной.

Одним из троянских коней проталкивания в высшую школу идеологии так называемой свободной траектории образования является парадигма «программирования», согласно которой «...хороший компьютер стоит всего тысячу долларов. И вот: сотня кнопок на клавиатуре — и пожалуйста: хочешь написать программу лучше, чем Microsoft или даже 1С, — пробуй!»

Иную точку зрения представил гость из Греции Диомидис Д. Спинеллис. Во главу инженерии программирования этот «греческий информатик» поставил знание предметной области, в которой ПО будет работать. По его мнению, основанному на богатой практике, на этом фундаменте открытая модель разработки позволяет правильно выбрать и быстро освоить инструментарий для программирования и тестирования приложений.

Уместно при этом вспомнить опыт системы образования в СССР, когда наряду с некоторым количеством экономистов общего профиля, подготавливаемых в университетах, существовала широкая система подготовки экономистов-отраслевиков на факультетах экономики в технических вузах, способных смолodu погрузить их в отраслевую специфику.

В новой России ситуацию поставили с ног на голову, призывая смолodu погружать инженеров и учёных в специфику бизнеса, основанного на примате принципов time to market и do it faster.

Возможно, для восстановления здравого смысла в ИТ-образовании (будем для определённости говорить только о нём) имеет смысл создать

Совместимость open-source-лицензий

образовательный аналог ФСТЭК и ему поручить, например, возродить культуру получения знаний в системе отечественного образования. Может быть, профессор Шалыто согласится возглавить такой «ФСТЭК для образования» и сформирует на базе, например, ИТМО соответствующий Центр возрождения ИТ-образования?

МЕЖДУ СЦИЛЛОЙ ИНТЕЛЛЕКТУАЛЬНОЙ ЩЕДРОСТИ И ХАРИБДОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Нельзя не согласиться с рамочным утверждением проекта «Стратегии...» о том, что «распространению открытого ПО в России препятствует ряд проблем», но вряд ли к ним уместно отнести «незнание юридических аспектов использования открытого ПО». ROSS 2021 показал, что немало представителей российского ИТ-сообщества ещё и дадут сто очков форы большинству юристов, специализирующихся в сфере защиты прав на продукты Open Source. При этом нельзя не упомянуть комментарий одного из спикеров дискуссии «о формировании инфраструктуры для открытого кода» о том, что лучшими юристами в этой сфере являются выпускники Физтеха.

Тем не менее невозможно отрицать, что юридические аспекты правовой защиты продукции на основе Open Source способны создать изрядную головную боль.

Один из таких аспектов — совместимость или несовместимость лицензий, «грибницей» которых опутан нынешний мир зарубежного пространства Open Source (см. рисунок). Подобная ситуация в условиях критичности для разработчиков параметров time to market и do it faster приводит к тому, что «юридические аспекты использования открытого ПО» нередко просто игнорируются.

Ситуация не безвыходная, и тут «есть два пути».

Первый — использование специализированных продуктов экосистемы инструментария DevSecOps для проверки совместимости лицензий.

Второй — совершенствование правовой базы использования Open Source.

По мнению ряда юристов (а согласно общему правилу, у двух юристов всегда существует три мнения), пока «в России нет чёткого понимания в области правовой регуляторики Open Source» и «в рамках действующих объектов интеллектуальной собственности Open Source не относится ни к одному из объектов».

При этом в жесточайшем кризисе находится не только мировая экономика, но и законодательство (международное и национальные) в сфере защиты так называемой интеллектуальной собственности. В связи с этим возможны и нестандартные решения, подобные недавно принятому закону о возможности выпуска в экстренных ситуациях

лекарственных препаратов без получения согласия правообладателя. Хотя оптимальным решением стала бы разработка законодательства на новых принципах, убирающего препоны ныне действующих законов о защите интеллектуальных прав на пути развития техники и технологий, культуры и экономики. Но где тот Анатолий Шалыто от юриспруденции, что мог бы возглавить процесс?

ОТ ТЕХНОЛОГИЧЕСКОГО ЦЕНТРА ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ ЯДРА LINUX К ЦЕНТРУ ТЕХНОЛОГИЙ БЕЗОПАСНОГО ПРОГРАММИРОВАНИЯ?

В 2021 году тема «безопасного программирования» неофициально стала одной из сквозных на конференции BISS 2021 и поднималась прямым текстом на обеих панельных дискуссиях, а её следы (или уши) можно было обнаружить в ряде докладов на практических секциях.

И хотя эксперты «панелей» BISS 2021 напирали на экономическую неэффективность внедрения «безопасного программирования», заместитель руководителя ФСТЭК дал твёрдый отпор фракции «экономистов» и набросал «эскиз» маршрутной карты инициатив и действий регулятора для поддержки «инжиниринга» «безопасного программирования».

Ждём круглого стола?



Марина БРОДСКАЯ
обозреватель BIS Journal

В ОЖИДАНИИ ШТУРМА

ENISA РЕКОМЕНДОВАЛО СОЗДАТЬ ЕДИНЫЙ ЕВРОПЕЙСКИЙ СТАНДАРТ ОБРАЗОВАНИЯ В ОБЛАСТИ ИБ

За последнее десятилетие сфера информационной безопасности значительно расширилась. Однако число специалистов в этой области не увеличилось, отмечается в отчёте Европейского объединённого агентства по кибербезопасности (ENISA).

ИССЛЕДОВАНИЕ

Дефицит квалифицированных специалистов разного уровня сказывается как на национальных рынках труда, так и на мировом. Испытывает нехватку кадров специалистов в сфере кибербезопасности в том числе и европейский рынок труда. Специалисты ENISA проанализировали тенденции в образовательных программах разного уровня и подготовили отчёт агентства «Решение проблемы нехватки навыков кибербезопасности в ЕС и пробелов в высшем образовании». В качестве базы они взяли 138 учебных программ высшего образования по кибербезопасности университетов 25 европейских стран и сделали прогноз перспектив на рынке труда.

Основные выводы оптимистичны: количество программ и студентов, получающих высшее образование в области ИБ, растёт. В ближайшие 2–3 года число выпускников — молодых специалистов увеличится вдвое. Наблюдается и гендерный перекос: на специальности ИБ поступает только 20% студенток.

Исследование учебных программ проведено в соответствии с Национальной системой оценки воз-

можностей (NCAF) Агентства ЕС по кибербезопасности (ENISA). Рассматривались не только осведомлённость, обучение, задачи и упражнения студентов. Система оценки также учитывала повышение квалификации кандидатов и обучение их новым навыкам, которые необходимы и востребованы на рынке труда.

РЕКОМЕНДАЦИИ УНИВЕРСИТЕТАМ

По итогам исследования специалисты ENISA дали следующие рекомендации университетам:

- ♦ увеличить количество учащихся и в итоге выпускников направлений ИБ за счёт диверсификации учебных программ, формата обучения и предоставления стипендий в вузах;

- ♦ разработать и поддерживать единый стандарт, работающий в правительстве, отраслях и учебных заведениях, путём принятия общей структуры, касающейся ролей, компетенций, навыков и знаний в области кибербезопасности; за основу предлагается взять европейскую структуру навыков кибербезопасности и продвижения навыков, задач и соревнований в области ИБ;

- ♦ развивать взаимодействие в области кибербезопасности между заинтересованными структурами в государствах — членах ЕС при поддержке европейских органов и проектов, финансируемых Евросоюзом;

- ♦ проводить анализ текущих потребностей и тенденций рынка ки-

бербезопасности для оценки масштабов проблем и разработки возможных мер по их решению;

- ♦ поддерживать использование и продвижение базы данных университетов Евросоюза CyberHEAD (Cybersecurity Higher Education Database), в которых развивается направление кибербезопасности, чтобы учитывать все программы высшего образования в области ИБ, отслеживать тенденции, следить за прогрессом и эффективностью инициатив в области кибербезопасности.

КАК ВЫПОЛНЯТЬ?

Кто должен стать целевой аудиторией стандарта? В первую очередь — страны — члены ЕС и европейские учреждения, заинтересованные в квалифицированных кадрах в области кибербезопасности и повышении роли высшего образования: высшие учебные заведения (вузы) ЕС, бизнес и промышленность, исследователи и академическое сообщество.

Помимо стандартизации программ и подходов к высшему образованию, ENISA предлагает иные меры по повышению квалификации кадров и развитию кибернавыков.

Это и мероприятия, направленные на поддержку и укрепление навыков и компетенций в области ИБ в различных секторах и на всех уровнях — от неспециалистов до высококвалифицированных профессионалов. Цель таких акций и мероприятий ENISA, согласованных с Планом действий в обла-



Отчёт Европейского объединённого агентства по кибербезопасности (ENISA). Источник: www.enisa.europa.eu

сти цифрового образования на 2021–2027 гг., — продвижение высшего образования в области кибербезопасности в ЕС, чтобы отреагировать на текущую нехватку кадров в области ИБ.

ENISA создала Специальную рабочую группу по разработке Европейской системы навыков кибербезопасности. Планируется собрать многопрофильную группу экспертов для создания гармоничной программы в экосистеме образования, обучения и развития персонала в области кибербезопасности, а также для разработки общей терминологии и единого языка в контексте навыков кибербезопасности. Также в планах Агентства — представить структуру, способную согласовать образование, обучение, развитие кадровых

ресурсов и концепции ИБ. В структуру войдут:

- ◆ уже работающая БД CyberHEAD;
- ◆ ежегодное мероприятие, проводимое Агентством по кибербезопасности ЕС для молодых специалистов European Cyber Security Challenge (ECSC), которое включает обмен мнениями и опытом, а также соревнования по ИБ;
- ◆ регулярные информационные кампании, проводимые под эгидой ЕС, например Европейский месяц кибербезопасности (ECSM).

В состав специальной рабочей группы по повышению уровня осведомлённости в области ИБ вошли пред-

ставители банков и организаций, образовательных, коммерческих и государственных структур, правоохранительных и правозащитных органов, знакомых с кибербезопасностью не понаслышке. В состав наблюдателей вошли представители ЕС, Европола и Европейского центра по борьбе с киберпреступностью. Организаторы надеются, что рабочая группа проведёт мозговой штурм и выдвинет новые идеи и решения для повышения общего уровня гигиены кибербезопасности и осведомлённости в области ИБ и страны Европы войдут в цифровое будущее в полной готовности ко всем неожиданностям, которые могут случиться в цифровом пространстве.

УГОЛ ЗРЕНИЯ

В США И ИНДИИ К ОНЛАЙН-ОБУЧЕНИЮ ОТНОСЯТСЯ ПО-РАЗНОМУ

Новостная лента начала января 2022 года была похожа на сводки с фронтов: за несколько новогодних дней ковид «выкосил» миллионы людей по всей планете и вернул забытые за осень и начало зимы понятия «карантин» и «удалёнка». В спор родителей и учителей о необходимости дистанционного обучения вмешались профсоюзы — при выборе формы образования приоритетным стал вопрос физической безопасности педагогов. А с другой стороны планеты дистанционное обучение сочли за благо, поскольку доступ к цифровым технологиям получили дети из глухомани.

США

В США с самого начала 2022 года был поставлен очередной рекорд: всего за сутки высококонтагиозным штаммом Omicron заболели более 1 млн человек. Среди заболевших много учителей, поэтому в окружных департаментах штатов заговорили о возвращении к дистанционному обучению. Многие родители и эксперты выразили протест против такого перехода, который, как

они считают, оказывает неблагоприятное влияние на обучение и психическое здоровье детей. Но способов противостоять пандемии нет: со 2 января не менее 5200 школ в 1200 округах по всем штатам объявили о нехватке учителей и персонала, и очные занятия были отменены на 1–2 недели.

Каждый штат самостоятельно принимает решение по переводу школ на дистанционное образование. В одних округах были продлены каникулы, в других срочно начали удалённые занятия, но, учитывая нехватку учителей, сделали гибкое расписание, включив в учебный процесс как уроки онлайн, так и самоподготовку.

Такой разницей в подходах не всегда приветствуют учителя: в то время как дети легко переносили коронавирус, смертность среди взрослого населения растёт. На защиту интересов педагогов встали профсоюзы. Например, в округе Чикаго (более 340 тыс. учеников) профсоюз учителей проголосовал за восстановление дистанционного образования и настаивал на строгих протоколах безопасности, включая более широкое тестирование школьников.

Чикагский союз учителей призвал 27 тыс. своих членов не посещать занятия и работать удалённо до 18 января, если только вспышка коронавируса не стихнет или профсоюз и округ не договорятся о новых протоколах очного обучения.

Лидеры профсоюза отмечают, что показатели вакцинации подростков в возрасте 12–17 лет из числа меньшинств особенно низки, что способствует распространению коронавируса. В свою очередь, окружные специалисты возражают против дистанционного обучения, которое оказалось опасным опытом и больше всего вредит ученикам из числа тех же национальных меньшинств.

В спор профсоюзов и округов по всем штатам пришлось вмешаться даже Администрации президента США. Белый дом продолжит настаивать на том, чтобы государственные школы оставались открытыми, в том числе в Чикаго.

ИНДИЯ

С 3 января в стране стартовала вакцинация подростков в возрасте 15–18 лет. Однако новая волна пандемии привела к немедленному закрытию школ и колледжей во многих штатах, как минимум до конца января, а то и до середины февраля. В части штатов в университетах и колледжах отменены занятия физкультурой, а все экзамены, в том числе отложенные ранее, проведут онлайн. В ряде регионов ученики 9–12 классов продолжают ходить в школы, но наполняемость классов не должна превышать 50%. Дошкольники и ученики 1–8 классов повсеместно перейдут в онлайн.

На этом фоне Национальный совет по образованию для государственных и частных школ, контролируемый и управляемый правительством Индии, и частный Совет по экзаменам на аттестат зрелости Индии должны определить даты выпускных экзаменов для учеников 10-х и 12-х классов. Испытания планируется провести во



Онлайн-урок в индийском штате Керала



втором семестре, где-то с середины февраля, где-то — в марте-апреле 2022 г.

Государственные и частные учреждения по стране перешли на работу с 50-процентным присутствием персонала на рабочих местах. Многие университеты отправили студентов по домам. Например, Индийский институт инженерных наук и технологий (IIEST) в Западной Бенгалии попросил студентов покинуть кампус и уехать домой, поскольку в штате отмечен резкий — от 50 до 70 % в день — прирост заболевших. В противном случае учащийся должен представить письмо от родителей с согласием на пребывание на территории университета. Студенты, оставшиеся в кампусе, должны соблюдать самоизоляцию, требования коменданта и посещать онлайн-занятия.

ИНДИЯ. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Казалось бы, индийские родители, как их коллеги из других стран, должны

протестовать, что многие дети третий год учатся онлайн, а учебные заведения даже не открывались для очного обучения. Однако в дистанционном образовании многие видят преимущества.

По мнению Санжайя Гоэла, директора Института инжиниринга и технологий Университета Дж. К. Лакшмипата, тенденции в области образовательных технологий полностью преобразуют учебный процесс. «Необходимо сделать онлайн-классы более увлекательными, с усилением человеческих связей через геймификацию и виртуальную реальность. Это сделает образование не только увлекательным, но и более доступным, гуманным и инклюзивным, — считает доктор Гоэл. — Очевидно, что современные тенденции в области образовательных технологий полностью трансформируют образовательный сектор. Новые технологии обучения будут дополнены искусственным интеллектом, технологиями машинного обучения и дополненной реальностью и

будут играть ключевую роль в образовании. Даже на сегодняшнем уровне студенты смогли продолжить совместное образование. Ожидается, что мировой рынок EdTech к 2026 г. составит \$ 240 млрд.

По словам Гоэла, геймификация станет одной из новых тенденций в образовании, которая будет доминировать в 2022 г. «Игровые уроки помогают вовлечь учащихся и вызвать у них максимальный интерес к учёбе. Даже использование видео для онлайн-обучения (или обучения на основе видео) получит новый импульс», — считает он.

«В ближайшие годы виртуальное обучение с улучшенной физической реальностью станет будущим образования, — полагает доктор Сильпи Саху, председатель Международной образовательной группы SAI. — Онлайн-обучение станет более реальным с помощью метавселенной, которая включит в себя концепцию дополненной и виртуальной реальности (AR и

VR). В 2021 г. уже были использованы широкоформатные виртуальные, почти реальные платформы для проведения школьных мероприятий. С появлением метавселенных онлайн-класс будет выглядеть более реальным, чем когда-либо. С переходом на дистанционное образование уже появились некоторые новые тенденции: персонализированное и темповое обучение, электронная оценка и использование технологий, улучшающих усвоение уроков и снижающих предвзятость оценок. По мнению Прашант Джейн, генерального директора издательства учебной литературы Oswaal Books, преподаватели будут использовать стратегии оценивания на основе приложений для оценки критического мышления.

Доктор Сильпи Саху также считает, что блокчейн поможет упростить утомительный процесс проверки и передачи заданий, записей о сотрудниках, уникальных учётных данных студентов, а также поможет избежать человеческих ошибок.

ИНДИЯ. ЖЕНЩИНА ТОЖЕ ЧЕЛОВЕК

В начале декабря Национальная комиссия по делам женщин (NCW) запустила онлайн-ресурсный центр (www.digitalshakti.org) для женщин. Его целью является обучение женщин азам кибербезопасности и безопасному использованию интернет-технологий. Это совместная инициатива NCW, Meta, CyberPeace Foundation и Autobot Infosec Pvt Ltd, представленная в рамках проекта «Переходим на цифру — цифровая Шакти 3.0».

Ресурсный центр призван служить источником информации и поддержкой в борьбе с кибернасилием в отношении женщин. Там представлена информация в различном формате.

♦ Информационные видеоролики на различные темы кибербезопасности. С их помощью в доступной форме любая женщина сможет оценить угрозы и принять меры предосторожности, узнает, как защитить себя в критической ситуации.

♦ Информационные баннеры — небольшие рисунки предназначены для быстрого обучения посетителей страниц. Они дают краткую информацию

по различным вопросам для учёбы «на лету».

♦ Справочный центр — это отдельный раздел Ресурсного центра, который предлагает помощь женщине, попавшей в беду, по вопросам, связанным с безопасностью в Интернете: кибербуллинг, киберпреследование, финансовое мошенничество, секс-вымогательство, шантаж и т.д.

Планируется создать отдельный раздел для консультирования, чтобы пострадавшая могла получить помощь в режиме реального времени. Фонд CyberPeace Foundation уже принимает заявки с сайта и быстро предоставляет консультации женщинам, нуждающимся в защите.

На страницах Ресурсного центра будет доступна и психометрическая оценка состояния человека. Женщина может пройти тест и получить оценку своего психического здоровья, при этом все данные тут полностью защищены и недоступны третьей стороне.

В разделе электронного обучения женщина может пройти уроки, изучить информацию по теме и получить оценку.

Раздел Ресурсного центра «Сообщения» предоставляет информацию обо всех способах сообщений о киберпреступлениях в отношении женщин. Этот раздел предоставит пользователям пошаговый процесс сообщения о проблемах киберпреступности и поможет самостоятельно решать множество проблем, таких как сообщение в социальных сетях, удаление контента с веб-сайтов, обращение в правоохранительные органы и даже возмещение ущерба.

В рамках первых этапов проекта We Think Digital — Digital Shakti 3.0 к проблемам кибербезопасности было привлечено внимание более 217 тыс. женщин по всей Индии. За второй год программы были проведены 167 семинаров, которые охватили 105 тыс. человек, включая студентов, преподавателей и социальных работников. Все они прошли обучение по темам поведения в глобальной сети Интернет, получили понятие о цифровом следе, ответственном поведении в цифровом пространстве, кибербезопасности и киберпреступниках, а также о методах борьбы с дезинформацией

и киберпреступлениями. Программа была номинирована на премию WSIS Prize 2020.

В рамках третьего этапа программы, который стартовал в марте 2021 г., планируется охватить порядка 1,5 млн женщин и девушек по всей Индии.

LIFELONG LEARNING STARTUET В ИНДИИ

Индийская UpGrad — крупнейшая компания высшего онлайн-образования в Азии — запускает краткосрочные курсы по кибербезопасности и аналитике данных. Две новые программы посвящены кибербезопасности и анализу данных, они предназначены для профессионалов, обладающих предметными знаниями. По окончании обучения обладатели сертификатов смогут добиться новых карьерных высот, считают разработчики учебных курсов.

Программа сертификации кибербезопасности рассчитана на 29 недель, а программа сертификации аналитики данных — на 36 недель. Оба курса были созданы UpGrad совместно с учебным центром Fullstack Academy из Нью-Йорка и Калифорнийским технологическим институтом и включают живые и записанные лекции, а также возможность учиться в процессе работы.

Комментируя старт новых учебных курсов, Фалгун Компалли, соучредитель UpGrad, отметил, что в связи с пандемией вырос спрос на облачные технологии, что потребовало от работников новых навыков и изменило потребности рынка труда.

Компания UpGrad постоянно оценивает потребности рынка и разрабатывает эффективные программы повышения квалификации, помогает справиться с общим кризисом спроса и предложений. Благодаря партнёрству UpGrad с американскими Fullstack Academy и Caltech учащиеся в Индии могут принять участие в практических онлайн-занятиях по аналитике данных или кибербезопасности, которые являются такими же строгими и качественными, как программы обучения в США. Это особенно важно для крупных корпораций и их региональных отделений, которые стремятся повысить квалификацию в быстро развивающемся технологическом ландшафте.

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ СТАНОВИТСЯ РЕАЛЬНОЙ УГРОЗОЙ

МИР И КИБЕРИНЦИДЕНТЫ — ГЛАЗАМИ СТУДЕНТОВ МГЛУ

Творческое сотрудничество BIS Journal со студентами-второкурсниками МГЛУ (ИНЯЗ им. Мориса Тореза) продолжается. Их задача — выбрать в СМИ разных стран сообщения о киберинцидентах и по возможности их прокомментировать. Эксперимент оказался успешным: редакция получила сотни случаев, из которых после фильтрации получился довольно насыщенный информационный коктейль — своеобразный гибрид дайджеста и обзора международной прессы. Продолжаем публиковать интересные примеры из студенческих работ.

ИРАН

9 июля 2021 года в Иране произошёл настоящий железнодорожный апокалипсис. Его причиной стал сбой в компьютерной системе одной из крупнейших железнодорожных компаний страны. Интересно, что на этот день были запланированы масштабные боевые учения, для проведения которых была необходима транспортировка боеприпасов и экипировки на военный полигон на юго-западе страны.

— Причиной транспортного коллапса стала кибератака, — заявил министр информационных и коммуникационных технологий Мохаммад Джавад Азари Джахроми Ирана (*подготовила по материалам иранских СМИ Гаряева Д.А.*).

Если хочешь найти преступника, ищи, кому выгодно. Кому же могла быть на руку такая кибератака? В первую очередь подозрения падали на давних противников Ирана, которые находятся с ним в перманентном конфликте, — США и Израиль. Ведь любой шаг Ирана назад для них — шаг вперёд. Выгоден ступор транспортной системы страны и соседствующему с Ираном Азербайджану, который тесно связан с ним железнодорожным сообщением.

Способом реализации киберугрозы стало вирусное вмешательство в работу компьютерной системы железнодорожной компании. В результате были сорваны военные учения и испытания новых типов оружия: в ситуации транспортного коллапса перемещение необходимых боеприпасов и оборудования стало невозможным. Военные учения перенесли. Однако в результате

кибератаки пострадали и тысячи жителей Ирана, так как железнодорожная компания осуществляет в основном гражданские перевозки.

«Поезда были задержаны или отменены из-за нарушений в работе билетных касс и веб-сайта национальной железной дороги, сбоя грузовых перевозок, а также «беспрецедентного хаоса на вокзалах по всей стране», — сообщила государственная телекомпания IRIB. Помимо прямой атаки на серверы компании, хакеры опубликовали на информационных табло на вокзалах и станциях номер телефона верховного лидера страны аятоллы Али Хаменеи в качестве номера, по которому можно позвонить для получения информации, что внесло дополнительные сложности в работу спецслужб.

ШВЕЙЦАРИЯ

В апреле 2021 г. правительство Швейцарии представило на обсуждение общественности проект нового «Доклада о положении в области безопасности — 2021». В случае его одобрения и согласования всеми ведомствами доклад планировалось вынести на одобрение парламента в конце 2021 г. (*подготовила Мария Кондрахина — по материалам swissinfo.ch (подразделение Швейцарской национальной теле- и радиокompании SRG SSR)*). Последний раз подобный документ принимался в августе 2016 г., однако с тех пор в мире многое изменилось, появились новые угрозы и опасности, при этом старые угрозы национальной безопасности остались теми же», — говорилось в сопроводительной записке к документу.

В докладе перечислены, в частности, приоритеты, которые должны находиться в основе политики безопасности Швейцарии. «География и политика





(расположение в центре Европы в окружении стран НАТО и политика нейтралитета) больше не защищают Швейцарию как раньше», — отметили создатели доклада. Новой основной угрозой для страны они посчитали кибернетические атаки и фейковые новости.

С точки зрения Федерального совета (правительства Швейцарии), новыми и серьёзными угрозами для страны стали кибератаки и прицельное распространение в социальных сетях и в интернете в целом заведомо ложной информации. «Это совершенно новые явления, которые всего за несколько лет стали особенно серьёзными вызовами и угрозами для государства, экономики и общества. Поэтому Швейцария должна ещё больше адаптировать свою политику безопасности к изменившимся условиям и новым угрозам».

По мнению Федерального совета, это не означает, что старые угрозы ушли в прошлое: «Конвенциональные (традиционные) вооружения и средства ведения войн вновь используются во всём мире в расширяющемся масштабе. Соответственно, такие средства обороны, как современные боевые самолёты, остаются незаменимыми инструментами обороны и обеспечения безопасности страны и её населения».

В Докладе об основах политики безопасности Федеральный совет определил девять основных целей, которые должны стать приоритетными для Швейцарии в ближайшие годы. Например, необходимо укрепить систему раннего обнаружения потенциальных угроз. Несколько целей Доклада

связаны с пандемией коронавируса и вызванным ей кризисом.

Ещё одна цель: «обеспечение условий для свободного формирования народом мнения по актуальным вопросам политической повестки и противодействия распространению искажённой информации, с тем чтобы общественные и политические дискуссии в Швейцарии проходили свободно, прозрачно, на основе фактов, а не фейков, при этом без дезинформации, без попыток пропаганды и влияния со стороны государственных органов власти».

В докладе, по мнению обозревателей, представлен трезвый взгляд на мир и геополитическую ситуацию: гонку вооружений, террористические организации, напряжённость между Россией и НАТО, увеличение количества вооружённых конфликтов на окраинах Европы. Угрозой является внешнее влияние, в частности, Россия и Китай часто упоминаются как источники кампаний по дезинформации, которые являются неотъемлемой частью так называемых гибридных войн. Федеральный совет опасается, что иностранные государства могут попытаться оказать влияние на граждан Швейцарии и, в частности, на результаты референдумов.

К каждой из девяти целей, указанных в тексте, Федеральный совет определил пакеты конкретных мер, которые должны быть реализованы в течение следующих нескольких лет.

В будущем планируется публиковать обновлённый «Отчёт о политике безопасности» раз в 4 года, в период между парламентскими выборами.

АВСТРАЛИЯ

В результате кибератаки были похищены личные данные 80 тыс. государственных служащих штата Южная Австралия. Эти сведения в начале декабря 2021 г. подтвердил казначей и член законодательного совета Южной Австралии Роб Лукас. По его данным, записи 80 тыс. государственных служащих были украдены в результате кибератаки, которая была проведена против компании Frontier Software. Этот подрядчик в течение последних 20 лет предоставлял программное обеспечение для расчёта заработной платы правительства Южной Австралии. Украденные сведения касаются сотрудников, работающих на правительство по состоянию на июль 2020 г. Не пострадали только данные Департамента образования.

Расследование инцидента продолжается, но считается, что он связан с атакой российских хакеров-вымогателей, произошедшей в ноябре 2021 г., пишет The Guardian. Украденная информация включает имена, фамилии сотрудников, дату рождения, номер налогового досье, домашний адрес и реквизиты банковского счёта. Среди пострадавших члены парламента и правительства Южной Австралии, сотрудники департаментов, советов и комитетов.

Всем пострадавшим рекомендовано принять меры безопасности, такие как смена паролей и контрольных вопросов, используемых для идентификации человека, отслеживание учётных записей на предмет любых необычных действий.

Роб Лукас отметил, что правительство не может немедленно расторгнуть контракт с Frontier Software, поскольку для поиска нового поставщика потребуется не менее полугода.

В свою очередь, генеральный директор Frontier Software Australia Ник Сауткомб заявил, что компания отслеживает любую подозрительную деятельность по мере продолжения расследования и активно сотрудничает со спецслужбами и клиентами. «Это первый подобный киберинцидент, с которым когда-либо сталкивалась компания Frontier Software. «Мы стремимся извлечь уроки из этого опыта и внедрить все необходимые меры

кибербезопасности, чтобы свести к минимуму вероятность возникновения инцидента в будущем», — заявил Сауткомб.

В уведомлении, размещённом на веб-сайте Frontier Software 9 декабря, компания сообщила, что 13 ноября некоторые из её австралийских клиентских систем пострадали в результате кибератаки. Об инциденте были проинформированы клиенты, Комитет по вопросам конфиденциальности Южной Австралии, Управление Комиссара по информации Австралии и федеральная полиция страны.

И. о. генерального секретаря Ассоциации государственной службы Наташа Браун заявила, что профсоюз обращается за юридической консультацией от имени своих членов. «Правительство должно взять на себя полную ответственность за целостность персональных данных, — считает Браун. — Профсоюз ожидает, что правительство покроет любые расходы для участников в связи с любыми неблагоприятными последствиями кражи данных, включая любые финансовые потери».

О компенсации за украденные данные говорит и Джастин Уоррен, председатель Electronic Frontiers Australia — австралийской некоммерческой организации, представляющей интересы пользователей Интернета в области сетевых прав и свобод. Он полагает, что инцидент «слишком знакомый» и пострадавшим должна быть выплачена компенсация за «работу, которую они должны выполнить, чтобы отреагировать на это нарушение их конфиденциальности».

«Этот инцидент ещё раз демонстрирует, что, как только правительство или бизнес получают ваши данные, вы мало что сможете сделать, если кибербезопасность недостаточно хороша, — считает Уоррен. — Правительства продолжают требовать, чтобы мы доверяли им наши данные, но я изо всех сил пытаюсь понять, почему кто-то это сделал. Если чиновники хотят нашего доверия, они должны его заслужить».

AMAZON

6 октября 2021 года платформа для стримов Twitch (сервис принад-



лежит компании Amazon Джеффри Безоса) потерпела самую крупную утечку данных в истории существования частных создателей развлекательного контента (подготовила по материалам СМИ Ульяна Едличка). Судя по первым сообщениям в Сети, в утечке содержался исходный код Twitch, внутренние SDK (набор средств разработки), внутренние инструменты Twitch, данные о заработке стримеров с 2019 г. и файлы проекта Vapor — предполагаемого конкурента Steam от Amazon Game Studios. Кроме самой платформы, пострадали и её пользователи, многие из которых не желают делиться сведениями о своих доходах с публикой.

Казалось бы, утекли важные данные и конфиденциальная информация. Однако инцидент не получил того отклика, на который, похоже, рассчитывал его автор: украденные данные и сведения заинтересовали только непосредственных участников и некоторых журналистов. По словам самих стримеров, их доходы непосредственно на платформе и так можно посчитать.

В документах, появившихся на имиджборде 4chan, перечисляются выплаты стримерам, в том числе известным, которые были сделаны с августа-сентября 2019 г. по октябрь 2021 г. Больше всех за этот период заработали стримеры CriticalRole, Canadian xQC и American Summit1g. Например, канал CriticalRole получил за этот период \$9,5 млн. Указанные цифры не

отражают реальных заработков стримеров, так как не включают доходы через спонсорство и другие платформы.

Автор утечки в своём посте на хакерском форуме отметил, что опубликовал лишь первую часть полученных данных, однако где и когда ждать следующей публикации, а также будет ли она выставлена на продажу, он не уточнил.

В корпоративном блоге Twitch факт утечки подтвердили, но отметили, что речь идёт о внешнем взломе системы из-за неправильной конфигурации на сервере. Данные банковских карт пользователей сервис не хранит. Сведений об утечке данных пользователей для входа на платформу (что критичнее) в компании Twitch не имеют.

Инцидент взволновал даже чиновников Роскомнадзора, которые потребовали от американской компании предоставить данные о скомпрометированном объёме личной информации российских пользователей Twitch, хотя никто из пострадавших не обращался с жалобами в контролирующее ведомство.

Сам автор «слива» заявил, что атака на сервис носила гуманитарный характер и причиной кражи данных и их публикации стала «токсичность» сообщества пользователей Twitch и желание усилить конкуренцию в сфере стриминговых сервисов.

Публикацию подготовила
Марина Бродская



Анна СЕЛЕЗНЕВА
аналитик Отдела
киберкультуры
Сбербанка

ПОМОГИ СЕБЕ САМ

КАК ПЕНСИОНЕРУ ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ

Нам часто кажется, что мошенники точно не смогут нас обмануть. Но нередко бывает так, что в самый ответственный момент осторожность и бдительность отходят на второй план, а мы попадаем на удочку злоумышленников. Чтобы эти ситуации навсегда остались в прошлом, необходимо уметь защищать себя от кибератак. Рассказываем, как распознать мошенника и не позволить ему украсть ваши деньги.

Необязательно быть специалистом в области кибербезопасности, чтобы уметь защищать себя и свои средства. И не надо быть продвинутым пользователем смартфона или компьютера. Главное — знать, где может таиться угроза, как избежать атаки мошенника и правильно её отразить. Для этого предлагаем не ждать помощи от детей и внуков, а прямо сейчас научиться защищать себя самостоятельно. Это несложно! Разберём несколько самых популярных ловушек, в которые аферисты могут пытаться заманить пенсионера.

Но прежде всего освежим в памяти базовые правила кибербезопасности:

- ◆ помните, сотрудник банка никогда не попросит вас продиктовать номер карты, код из СМС или секретный код на обороте карты (CVV);
- ◆ никогда не выполняйте действия под диктовку незнакомцев, даже если они представляются сотрудниками служб безопасности банков или правоохранительных органов;
- ◆ всегда сообщайте банку о мошеннике, если столкнулись с ним в Сети или по телефону;
- ◆ проверяйте реквизиты переводов и платежей, которые приходят в СМС;
- ◆ не переходите по подозрительным ссылкам в СМС и письмах;
- ◆ устанавливайте приложения только из официальных магазинов.

СХЕМА № 1: ОБМАН ПО ТЕЛЕФОНУ

История: рано утром Алексей Михайлович был на рыбалке. Неожиданно зазвонил телефон, человек на другом конце провода представился сотрудником полиции и сообщил мужчине, что его внук был пойман с партией наркотиков. Чтобы урегулировать вопрос, нужно прямо сейчас отправить на карту крупную сумму.

В чём опасность: главный «союзник» мошенников — сильные эмоции. В этом случае

преступник может запугивать вас, практически доводить до паники, перечисляя все ужасы, которые якобы могут случиться с вашим родственником. Злоумышленник вводит вас в стрессовую ситуацию (а в ней мыслить здраво практически невозможно) и настаивает на быстром действии — переводе денег. Иногда мошенникам удаётся выманить у пенсионеров по несколько сотен тысяч рублей.

Что ещё может говорить телефонный мошенник:

- ◆ «Здравствуйте, это служба безопасности банка, по вашей карте обнаружена подозрительная активность, необходимо отменить операцию. Для этого продиктуйте мне полный номер карты и срок её действия»;
- ◆ «Вам положена компенсация (выплата, государственная субсидия). Чтобы её получить, оплатите небольшую комиссию»;
- ◆ «Добрый день! Недавно вы проходили обследование в поликлинике. Ваш диагноз требует немедленного лечения. Мы готовы привезти вам необходимые лекарства и оборудование, которое вы сможете купить по самой выгодной цене».

Как защититься:

Прежде всего возьмите паузу, с какой бы новостью вам ни позвонили. Не совершайте никаких операций с деньгами под диктовку незнакомцев.

Если вам сообщили о том, что друг или родственник в беде, попытайтесь связаться с ним или его близкими. Если предложили получить компенсацию — перепроверьте информацию на портале Госуслуг. А по поводу здоровья консультируйтесь с лечащим врачом, а не с телефонными мошенниками.

Кроме того, настройте проверку телефонного номера при входящем звонке в мобильном приложении СберБанк Онлайн. Система определит, является ли абонент жуликом, и предупредит вас об этом. Чтобы включить функцию, на главном экране приложения выберите раздел «Безопасность», далее перейдите по строчке «Проверка входящих звонков» и нажмите на кнопку «Подключить».

И помните, что сотрудники банка не запрашивают полный номер карты, срок её действия и трёхзначный код на обратной стороне. У них есть вся необходимая информация.

СХЕМА № 2: КОВАРНЫЕ СМС

История: Лидии Павловне пришло СМС: «Я ошибся в одной цифре номера телефона при регистрации на сайте. Вам должен был прийти код подтверждения. Перешлите его мне, пожалуйста. Извините за беспокойство!».

В чём опасность: вполне возможно, что сообщение прислал мошенник, который пытается получить доступ к вашему личному кабинету банка. Если вы «войдёте в положение» злоумышленника и перенаправите ему код, он сможет получить доступ к вашему онлайн-банку и украсть все деньги.

Как ещё может выглядеть СМС от мошенника:

- ♦ Сообщение с номера, похожего на телефон вашего мобильного оператора: «На ваш счёт зачислено 500 рублей». Ещё одно СМС сразу после первого: «Я по ошибке перевёл вам деньги. Верните их на номер 8 9XX-XXX-XXX-X»;

- ♦ «Ваша карта заблокирована. Для разблокировки позвоните по номеру 8 9XX-XXX-XXX-X» (рис. 1);

- ♦ «Оплата покупки на сумму 10 315 рублей успешно выполнена. Если вы не совершали операцию, обратитесь в службу безопасности банка по телефону 8 9XX-XXX-XXX-X»;

- ♦ «Вы стали победителем Всероссийской государственной лотереи. Чтобы получить приз, оплатите комиссию по ссылке».

Как защититься: к любым СМС с незнакомых номеров стоит относиться с подозрением, особенно если в них вас просят куда-то перезвонить или перейти по ссылке. Велика вероятность того, что, сделав это, вы или свяжетесь с мошенником, который начнёт «обрабатывать» вас, или попадёте на поддельный интернет-сайт (если ввести на нём свои платёжные данные, можно потерять деньги).

Если вам пришло сообщение о том, что с вашего счёта якобы списана крупная сумма, не спешите паниковать. Возьмите паузу, сделайте глубокий вдох и выдох и перезвоните в свой банк по номеру телефона, указанному на карте, чтобы уточнить информацию.

Помните, что бесплатный сыр бывает только в мышеловке, а люди не всегда оказываются теми, за кого себя выдают. Будьте бдительны с незнакомыми отправителями, которые говорят, что якобы ошиблись номером. Не пересылайте им информацию, которую они просят, а посоветуйте обратиться в банк или службу поддержки сайта, на котором произошла «ошибка».

А чтобы наверняка обезопасить себя от кражи денег с карты, установите суточный лимит трат в приложении СберБанк Онлайн. Для

этого в разделе «Безопасность» выберите опцию «Настройте безопасность», а дальше — пункт «Изменить суточный лимит».

СХЕМА № 3: ПОДДЕЛЬНЫЕ ИНТЕРНЕТ-САЙТЫ

История: Валентина Степановна давно хотела купить электрический культиватор, чтобы быстрее полоть грядки на даче. Однажды во время проверки электронной почты женщина увидела рекламу, в которой желанный прибор продавался с большой скидкой — за 5 тысяч рублей вместо прежних 15. Пенсионерка перешла на сайт, там ей предложили срочно заполнить заявку на покупку, чтобы забронировать культиватор, так как желающих его купить гораздо больше, чем самих инструментов.

В чём опасность: неправдоподобно выгодные предложения в интернете часто оказываются обманом. Как правило, поддельные, или фишинговые, сайты призывают потенциального покупателя молниеносно принять решение — якобы такой уникальный товар по такой привлекательной цене вы больше не найдёте нигде и никогда. Мошенники снова пытаются заставить вас действовать без раздумий и оставить на сайте платёжные данные — полный номер карты и трёхзначный код на обратной стороне карты, чтобы потом украсть деньги. А мы снова рекомендуем взять паузу и всё перепроверить.

Как ещё могут выглядеть электронные письма от мошенников и поддельные интернет-сайты (рис. 2):

- ♦ «Ваш адрес выбран победителем лотереи Международной корпорации лотерей. Чтобы получить вознаграждение в размере 300 тысяч рублей, перейдите по ссылке и заполните форму»;

- ♦ «Данные вашего счёта давно не обновлялись. Пожалуйста, перейдите по ссылке и оставьте актуальную информацию для корректной работы сервиса. В случае невыполнения требования вам грозит штраф в размере 10 тысяч рублей. Служба безопасности банка»;

- ♦ «Беспроеигрышные ставки на спорт! Ставьте на любимую команду и получайте деньги. Чтобы начать выигрывать, заполните форму».

Как защититься: если вы нашли товар, который давно искали, по низкой цене, внимательно изучите сайт. Вверху слева в адресной строке браузера должен быть значок в виде замочка и надпись «защищённый режим», а адрес в поисковой строке должен начинаться на <https://>. Эти детали говорят о том, что сайт настоящий (рис. 3).

Дополнительно сайт можно проверить в разделе приложения СберБанк Онлайн «Поддержка» — «Ваша безопасность».

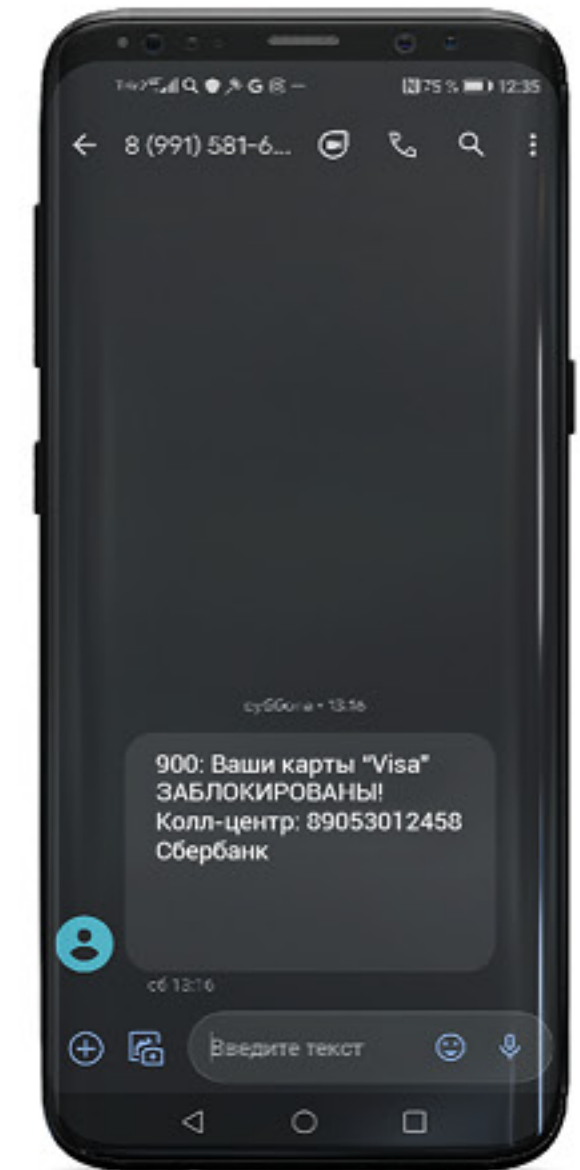


Рисунок 1. СМС от мошенника

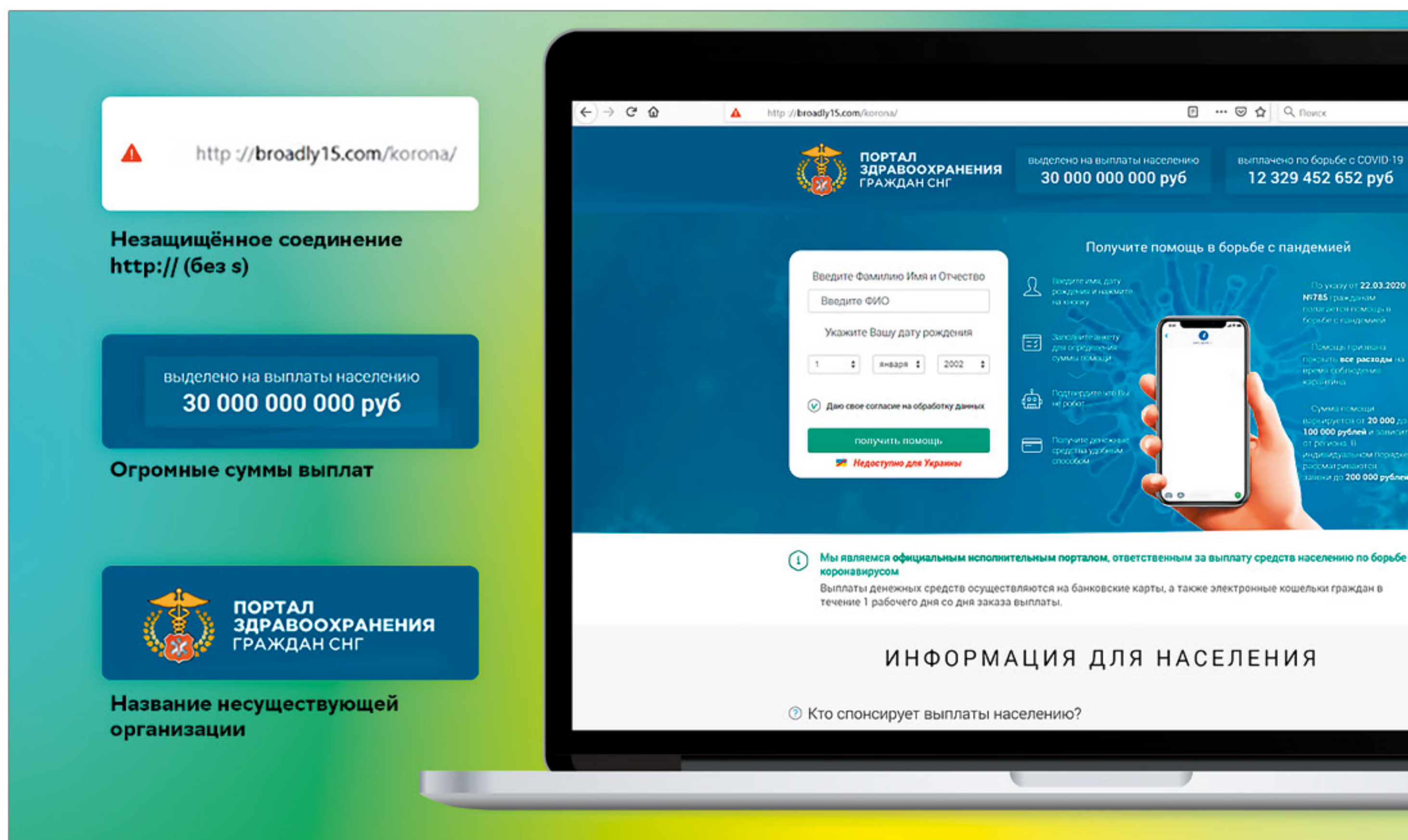


Рисунок 2. Типовой мошеннический сайт

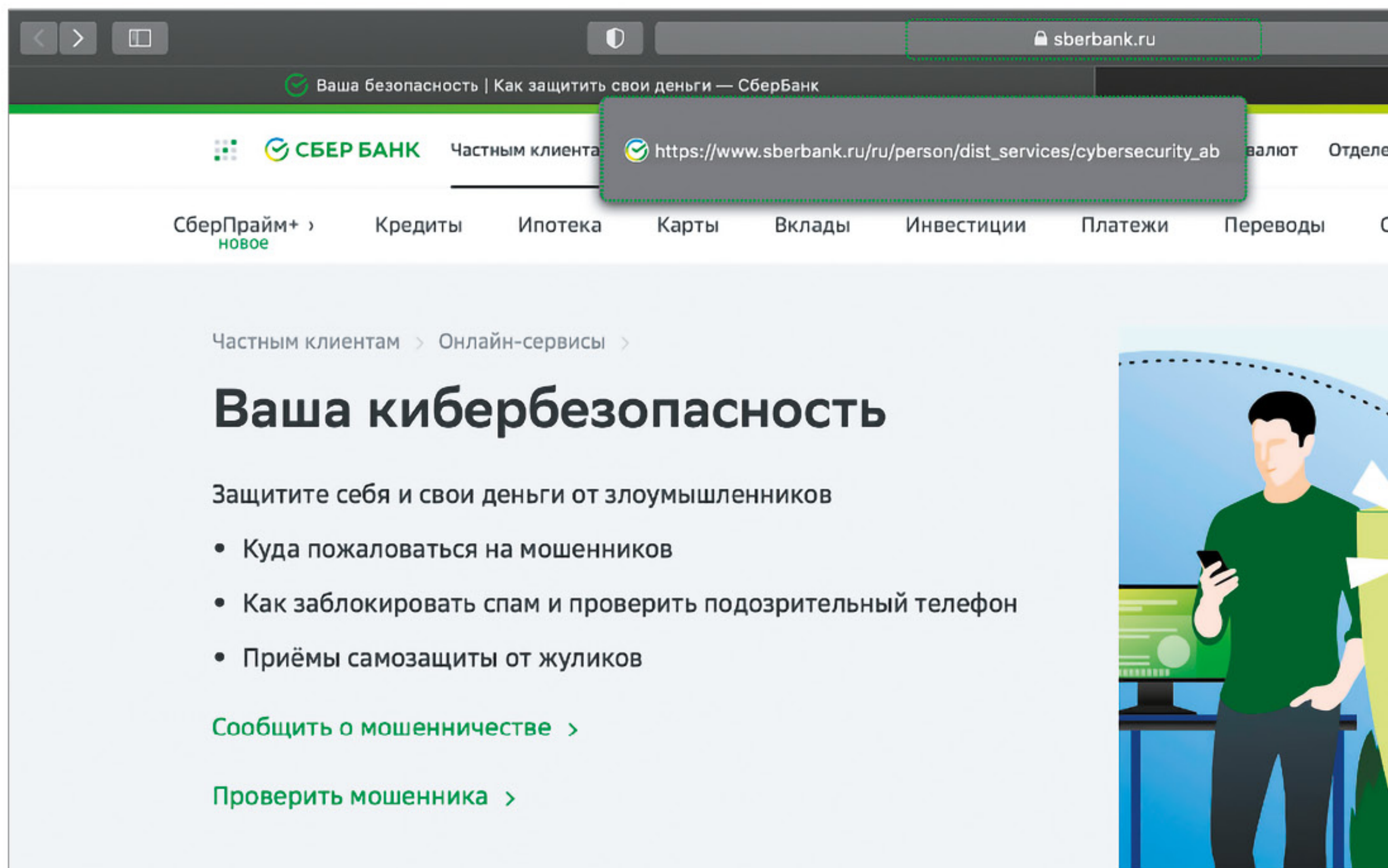


Рисунок 3. Официальный сайт (правильный адрес сайта начинается с https://, есть знак закрытого замка)

Программа подскажет, принадлежит ли сайт злоумышленникам, и даст рекомендации.

Кроме того, стоит насторожиться, если вас буквально вынуждают действовать быстро, сообщая, что акция вот-вот закончится и вы не успеете купить нужный товар.

ПОДУМАЙТЕ О БЕЗОПАСНОСТИ ЗАРАНЕЕ

Даже если вы не сталкивались с мошенниками и абсолютно уверены в своих знаниях кибербезопасности, нелишним будет установить в личном кабинете банка настройки, которые не позволят злоумышленникам добраться до ваших денег.

Настройте доступность счёта или вклада в удалённых каналах обслуживания. В приложении СберБанк Онлайн выберите счёт или вклад на главном экране приложения, затем перейдите в «Настройки» и в строчке «Скрыть» выберите опцию «Скрыть счёт везде». В этом случае операции по нему можно будет проводить только в офисе банка. Восстановить доступность счёта или вклада в удалённых каналах обслуживания возможно только при личном посещении офиса.

Установите суточный лимит расходов и операций по карте. Настройка позволяет ограничить сумму перевода и платежей, которую можно использовать за день. Например, вы знаете, что обычно не тратите и не переводите больше, чем две тысячи рублей в сутки. Если всё же нужно будет превысить этот лимит, потребуется звонок в банк. А такую проверку не пройдёт даже самый опытный жулик.

Чтобы изменить лимит, в разделе «Безопасность» выберите опцию «Настройте безопасность», а дальше — пункт «Изменить суточный лимит». В этой вкладке можно выставить необходимую сумму, а если вы захотите снова её

увеличить, просто позвоните в банк и подтвердите действие.

Полезная настройка **«ограничение на оплату в интернете»** поможет сделать безопасной оплату товаров и услуг онлайн. Чтобы максимально защитить деньги, стоит отключить возможность платить за покупки онлайн и вместо этого при оформлении заказов выбирать оплату картой курьеру (или в пункте выдачи). Если не установить такое ограничение, любой, кто знает полный номер вашей карты, срок действия и трёхзначный код безопасности с оборота карты, сможет оплачивать ей товары в интернет-магазинах, которые не требуют подтверждения по СМС.

А чтобы быть во всеоружии в случае встречи с мошенником, **изучите полезные материалы** на странице «Ваша безопасность» сайта sberbank.ru. Памятки, чек-листы и тесты расскажут, как распознать афериста по телефону и в интернете, как безопасно оплачивать покупки и услуги картой и на что стоит обращать внимание при использовании онлайн-сервисов — знать всё это необходимо для того, чтобы не стать жертвой киберпреступления.

О самых распространённых схемах обмана можно узнать в канале «Осторожно, мошенники!». В строке поиска наберите слово «осторожно», а дальше система сама найдёт канал (рис. 4).

А если всё-таки вас пытались атаковать, оставьте номер телефона или адрес сайта в специальном разделе «Сообщить о мошеннике» в мобильном приложении в разделе «Связь с банком». Сообщить о мошеннике можно и на сайте sberbank.ru — в разделе «Поддержка» — «Ваша безопасность». Там же можно проверить, принадлежит ли номер телефона или сайт злоумышленникам — система оценит опасность и подскажет, как действовать (рис. 5).

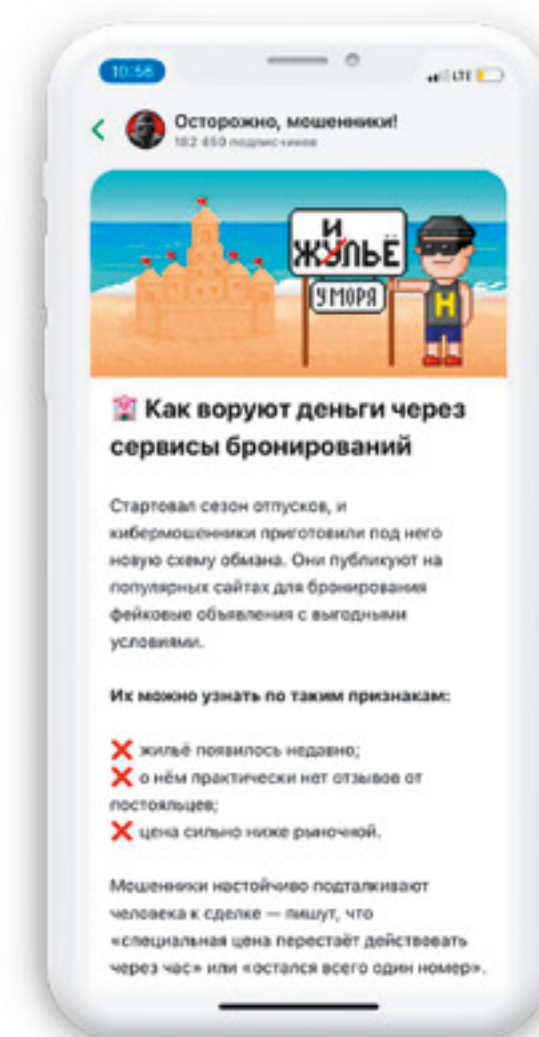


Рисунок 4. Канал «Осторожно, мошенники!» в СберБанк Онлайн

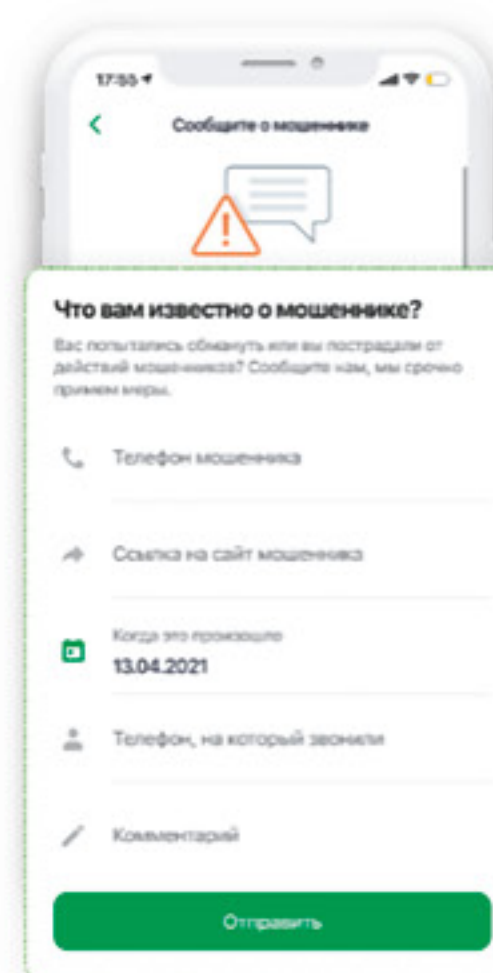


Рисунок 5. «Сообщить о мошеннике» — форма обратной связи в СберБанк Онлайн

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

1. Если вам звонят и говорят, что ваш друг или родственник попал в беду, а для помощи ему нужно отправить деньги, положите трубку и перезвоните человеку, о котором идёт речь.

2. Всегда берите паузу после того, как получите любую информацию от незнакомого человека — по телефону, СМС или в письме. Не отвечайте сразу, обдумайте ситуацию, предположите, в чём может быть риск, и только потом примите решение. И помните: деньги и спешка несовместимы.

3. Будьте осторожны с электронными письмами с вложенными файлами — они могут содержать вирусы. Перед тем как открыть, целесообразно предварительно проверить файл с помощью антивируса.

4. Не переходите по ссылкам, присланным в письмах с незнакомых адресов, особенно если вас призывают действовать как можно быстрее. А если всё-таки перешли, удостоверьтесь в безопасности сайта (найдите значок в виде замочка и <https://>).

5. Не заполняйте формы и анкеты, полученные по СМС или электронной почте с незнакомых номеров и адресов. Личные данные безопасно вводить исключительно на проверенных сайтах.

6. Чаще звоните более молодым родственникам и рассказывайте о звонках и сообщениях от незнакомцев, обращайтесь к ним за советом в ситуациях, вызывающих подозрение.



**Андрей
ЖАРКЕВИЧ**
эксперт BIS Journal

ОГРАБЬ МЕНЯ!

КАК ЗАЩИТИТЬ ОБЫЧНЫХ ЛЮДЕЙ ОТ КРАЖИ ДЕНЕГ ПО ТЕЛЕФОНУ

Вряд ли сейчас можно найти человека, который не слышал о телефонных мошенниках, опустошающих банковские счета физических лиц. Кажется, что их приёмы рассмотрены и объяснены во всех вариантах, поэтому не должны срабатывать. Однако статистика говорит о другом. По данным следственного департамента МВД России, ущерб от телефонного мошенничества в России за 11 месяцев 2021 года составил 45 млрд рублей. Половина потерпевших добровольно передавали преступникам секретные данные, пароли и коды.

Попробуем разобраться, откуда взялось это противоречие, какие меры предлагает регулятор и помогут ли они защитить граждан.

ИСТОРИЯ ОБМАНА

Рассмотрим мошенническую многоходовку с несколькими участниками.

Всё начинается со звонка от «сотрудника» службы безопасности банка. «Сотрудник» в довольно грубой манере сообщает, что проводит проверку личности клиентов банка и для подтверждения жертва должна назвать ему свои полные паспортные данные и реквизиты всех карт банка. Когда возмущённая жертва отказывается сообщить конфиденциальную информацию, собеседник говорит что-то оскорбительное и вешает трубку. Главная задача этого разговора — вызвать негативные эмоции у жертвы.

Через несколько дней жертва получает ещё один звонок. На этот раз с ней разговаривает «сотрудник внутренней безопасности Банка России», который спрашивает, звонили ли жертве из банка со странными вопросами, а затем сообщает, что проводится расследование деятельности недобросовестных сотрудников банка, и просит оказать содействие следствию.

Вскоре поступает ещё один звонок от «представителя Следственного комитета РФ», «майора отдела ФСБ по расследованию банковских преступлений» или какого-то другого представителя силовых ведомств со звучной должностью. Его служба расследует мошеннические инциденты с участием сотрудников банка, в частности прозвоны клиентов с требованием подтвердить паспортные данные. Чтобы поймать и наказать преступников, нужна помощь жертвы.

Помощь может быть самой разной. Например, жертве предлагают перевести деньги со своих счетов на «помеченный» защищённый счёт или передать наличные «надёжному человеку», который положит их в «спехранилище». Встречаются и варианты с оформлением кредита и передачей всей суммы «агенту ФСБ под прикрытием» или даже с продажей квартиры и размещением денег на «спецсчёте в ЦБ РФ». Во всех случаях мошенники обещают жертвам достойное вознаграждение после поимки преступников.

В обязательном порядке от жертв требуют соблюдения секретности, объясняя его тайной следствия, а иногда и угрожая ответственностью за разглашение.

КТО ПОД УДАРОМ?

Довольно распространено мнение, что мошенники обманывают только совсем наивных или неграмотных людей, далёких от реалий сегодняшнего дня. Но на самом деле всё гораздо серьезнее.

♦ В ноябре 2020 года бывший замначальника Следственного департамента МВД Дмитрий Какошин попался на уловку аферистов и предоставил им доступ к банковским картам. С его счетов списали 613 тысяч рублей. Генерал сообщил коллегам, что «находился под убеждением и психологическим воздействием».

♦ В 2020 году женщина 54 лет отдала мошенникам 400 млн рублей. «Спасая» свои сбережения, она в течение месяца снимала деньги со счетов и переводила их мошенникам.

♦ В мае 2021 года руководитель отделения психического и поведенческого расстройства НИИ им. Сербского, который проводит экспертизы убийц и маньяков, сняла со своих счетов 60 тысяч долларов США, 90 тысяч евро, 25 тысяч рублей, потом ещё 45 530 евро и 14 431 доллар США, а затем передала «специальному человеку» в кафе.

Генерал МВД или профессор психиатрии просто в силу своих профессиональных знаний не должны были поддаваться обману. Они совершенно точно знали о мошенниках и имели представление о сценариях, которые те используют. Однако, когда они сами стали участниками «спектакля», не смогли включить рациональное мышление и выпутаться из ситуации без потерь.

ПОЧЕМУ ЛЮДИ ВЕРЯТ АФЕРИСТАМ

Мошенники строят свои сценарии с учётом особенностей человеческой психики. Они знают, что сильные эмоции выводят человека из равновесия и отключают критическое мышление. Поэтому первое действие во всех сценариях — удар по базовым эмоциям — страху, гневу, радости, любопытству и т.п.

В описанном выше мошенническом сценарии первый удар по эмоциям наносит фальшивый сотрудник банка, вызывая у жертвы гнев и негодование.

Появившийся на втором этапе «сотрудник ЦБ РФ» снова атакует эти эмоции, заставляя жертву вспомнить о неприятном эпизоде. И сразу же даёт надежду на то, что преступников могут поймать и наказать, нужно всего лишь помочь следствию.

Для реализации этой надежды в дело вступает «следователь», который выполняет дальнейшую обработку жертвы. Он продолжает стимулировать сильные эмоции, усиливая их воздействие авторитетом. Для этого упоминаются ФСБ, Следственный комитет и Центральный банк РФ, а также «солидная» должность звонящего.

Ещё один фактор, который используют мошенники для повышения эффективности воздействия, — изоляция жертвы от родственников, друзей и знакомых. Они добиваются этого с помощью «режима секретности», запрещая сообщать кому-либо об участии в «расследовании». Не имея возможности посоветоваться с другими людьми, жертва остаётся под «очарованием» мошенников и выполняет нужные им действия.

Примечательно, что преступники уже вовсю используют борьбу с самими собой как дополнительную мотивацию для жертв: «Вы же слышали о телефонных мошенниках? Вы можете помочь поймать одну такую банду и получить вознаграждение! Вот что от вас требуется...» Желание помочь и жажда вознаграждения часто оказываются решающими факторами в деле убеждения жертвы.

Таким образом, практически все мошеннические кампании построены примерно по одной схеме: удар по базовым эмоциям → отключение рационального мышления жертвы → повышение интенсивности воздействия с помощью эмоциональных усилителей → доверие жертвы → профит.

К сожалению, практически все люди в большей или меньшей степени уязвимы для таких атак. Даже если в отдельных случаях они успешно распознавали звонки мошенников, другие сценарии всё ещё могут сработать.

КАК ПЫТАЮТСЯ ЗАЩИТИТЬ ГРАЖДАН

Огромные суммы хищений со счетов граждан не остались без внимания банковского сообщества, регулятора и правительства. Чтобы защитить владельцев счетов от мошенников, предлагают:

- ♦ дополнительную верификацию при денежных переводах и выдаче займов. Она должна предотвратить оформление кредитов и займов на человека без его ведома и стать препятствием для телефонных мошенников;

- ♦ обязательное двухфакторное подтверждение на портале госуслуг при идентификации заёмщика. Предполагается, что в этом случае злоумышленникам сложнее будет получить заём под чужим именем, поскольку, кроме логина и пароля от «Госуслуг», потребуется код из SMS;

- ♦ дать гражданам возможность самим решать, нужно ли им подключение дистанционных каналов доступа к банковскому счёту;

- ♦ дать возможность пользователям мобильного банка и других цифровых банковских услуг скрывать счета, вклады или карты в мобильном приложении и устанавливать ограничения по параметрам операций;

- ♦ сервис «второй руки» — возможность назначить другого клиента этого же банка своим помощником. Такой помощник будет получать уведомления о планируемых операциях с использованием цифровых каналов и сможет подтверждать или отклонять их, если заметит необычную активность. Инициировать подключение сервиса может только сам клиент, а при получении запроса на отключение такой услуги банкам рекомендуется проверять просьбу на предмет потенциального мошенничества.

БУДУТ ЛИ РАБОТАТЬ ЭТИ МЕРЫ ЗАЩИТЫ?

Фундаментальная проблема всех перечисленных мер состоит в том, что они не принимают в расчёт то, что практически во всех эпизодах с мошенниками люди действовали ДОБРОВОЛЬНО. Они ЗНАЛИ, что нельзя никому сообщать CVV-код банковской карты или SMS-код подтверждения операции. И уж точно они ПОНИМАЛИ, что, передавая деньги лично в руки незнакомым людям, рискуют лишиться их. Но это знание их не остановило. Мошенники сумели привлечь их к участию в спектакле и убедить добровольно расстаться с деньгами.

Предположим, что банки ввели обязательную дополнительную верификацию для перевода средств. Пусть, например, кроме SMS-кода, требуется принять звонок от робота и сказать: «Подтверждаю перевод». Как поступит человек,

Чтобы защититься от мошенников, клиенты должны не только знать о них, но и уметь действовать безопасно

который выполняет перевод денег, считая, что спасает их от преступников? Скорее всего, он подтвердит перевод точно так же, как буквально минуту назад добровольно сообщил код подтверждения мошенникам.

Аналогичная ситуация и с другими защитными мерами. Клиент банка должен иметь возможность управлять своими счетами. А значит, даже обязательный визит в офис банка не станет препятствием для мошенников, ведь они вполне могут убедить жертву, что сотрудники банка пытаются её ограбить.

КАК ВСЁ-ТАКИ ЗАЩИТИТЬ ЛЮДЕЙ?

Телефонные мошенники грабят клиентов банков, не применяя сложных технических средств. Они используют в качестве оружия социальную инженерию, эксплуатируют слабости людей, которые сформировались за годы эволюции. В результате жертвы самостоятельно обходят все системы защиты банков, считая, что действуют себе во благо.

Чтобы остановить мошенников, нужно в первую очередь работать с потенциальными жертвами — клиентами банков. Как показывает

практика, даже широчайшего информирования недостаточно, чтобы люди перестали верить аферистам. А как показывают описанные выше инциденты, даже те, кто знает и вроде бы не должен верить, всё-таки становятся жертвами. Причина в том, что, кроме знания, необходимы навыки безопасного поведения в различных ситуациях.

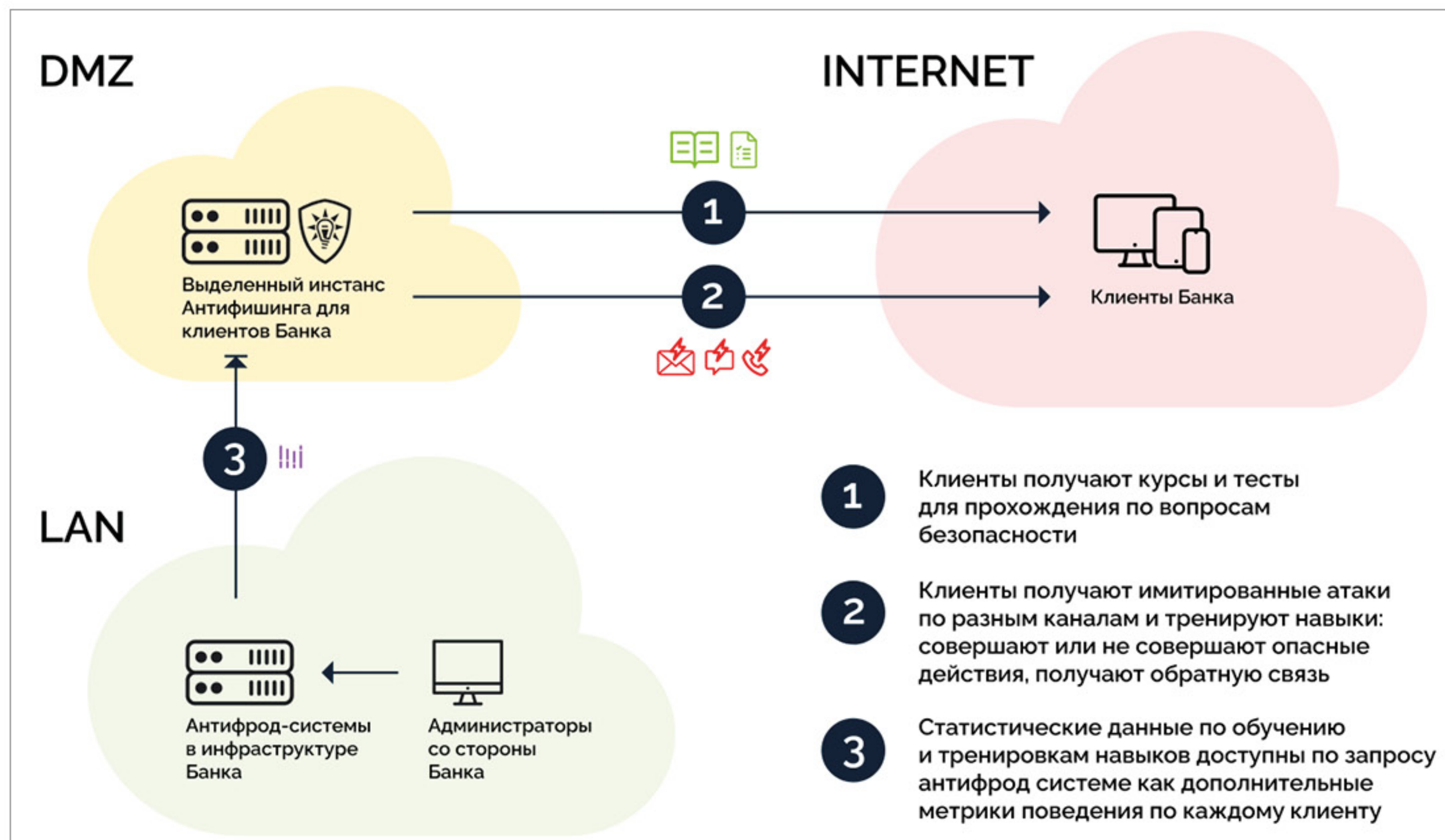
Многие банки используют оповещение клиентов — физических лиц о мошеннических угрозах, но, как и любое информирование, само по себе оно малоэффективно. Чтобы помочь банкам защитить своих клиентов и снизить операционные и репутационные риски, компания «Антифишинг» разработала решение «Антифрод», которое гибко встраивается в бизнес-процессы кредитной организации.

ОБ АНТИФРОДЕ

Система построена на технологиях «Антифишинга», показавших свою эффективность в выработке навыков безопасного поведения сотрудников компаний, но адаптирована к особенностям целевой аудитории — физических лиц — клиентов финансовых организаций (рис. 1).

В «Антифроде» реализован цикл обучения и тренировки навыков, который позволяет сформировать высокий уровень осведомлённости клиентов финансовых организаций и научить

Рисунок 1. Схема работы решения «Антифрод» от «Антифишинга»



их безопасному поведению в различных ситуациях (рис. 2).

В «Антифрод» имеется функциональность для обучения и тренировки навыков внешних пользователей в виде электронных обучающих курсов и диалоговых тестов, а также интерактивный тренажёр по безопасности и буклеты по безопасной работе в системе онлайн-банкинга, социальных сетях, мессенджерах и электронной почте (рис. 3).

Система «Антифрод» позволяет проводить имитированные атаки через СМС и по электронной почте с вложениями и фишинговыми сайтами. Решение может быть интегрировано с антифрод-системами и другими внутренними системами банков.

Таким образом, после внедрения «Антифрода» банк получит:

- ♦ улучшенную точность выявления мошеннических операций внутренними антифрод-системами благодаря сбору дополнительной информации о поведении клиентов;
- ♦ вместо множества клиентов-жертв — киберчемпионов, которые *не только знают*, как безопасно работать в цифровой среде, *но и умеют* защищать себя и свои деньги от мошенников (рис. 4).

ИТОГИ

1. Жертвами мошенников могут стать даже информированные люди, которые не только слышали про эту угрозу, но и занимаются борьбой с ней.
2. Больше половины жертв мошенников добровольно выполняли их указания, в том числе обходили меры защиты или даже снимали наличные средства и передавали их преступникам лично.
3. Эффективность мошенников объясняется эксплуатацией особенностей человеческой психики — воздействием на базовые эмоции (страх, гнев, любопытство) и использованием эмоциональных усилителей в виде срочности и авторитета.
4. Чтобы защитить клиентов, нужно вырабатывать у них навыки безопасного поведения в сложных ситуациях.
5. Добиться такого результата позволит сочетание информирования и систематической тренировки навыков с помощью имитированных атак.
6. Система «Антифрод» на технологиях «Антифишинга» позволяет реализовать все необходимые шаги для обучения, тренировки и контроля навыков клиентов и гибко интегрировать эти задачи в бизнес-процессы кредитной организации.



Рисунок 2. Цикл обучения и тренировки навыков в системе «Антифрод»

Вы платите картой в кафе

Официант проводит вашей картой по терминалу и просит ввести пин-код. После этого терминал распечатывает чек, на котором написано, что нет связи с банком. Официант извиняется и предлагает попробовать другой терминал, который находится у бара.

Отдать карту, пусть пробует	Попросить принести другой терминал
-----------------------------	------------------------------------

Рисунок 3. Пример теста из интерактивного тренажёра в составе «Антифрода»

1. Уровень знаний - Не обучался ○ - Прошел обучение ● - На обучении ▤ - Не прошел обучение вовремя ●	2. Уровень навыков - Выдержал атаку ● -5⁻² - Сообщил об атаке ○ 2⁻¹ - Открыл письмо ● - Перешел по ссылке или открыл файл ● - Ввел данные в форму ●
3. Опасные уязвимости ПО .NET 3.0 версий 3.0.30729 и ниже - Shockwave Flash версий 23.0 r0 и ниже	можно использовать в дополнение к существующим методам фишингпринтинга 1014 -213

Рисунок 4. Дополнительные метрики для антифрода по каждому клиенту



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

СОРОКОВЫЕ, РОКОВЫЕ... И СОЗИДАТЕЛЬНЫЕ

ОТ ПРИКЛАДНЫХ ЗАДАЧ В ОБЛАСТИ ШИФРОВАНИЯ
К ФУНДАМЕНТАЛЬНОЙ НАУКЕ

Если в Первой мировой войне криптографический фронт лишь впервые заявил о себе, что прозвучало хотя и ярко, но не слишком громко, то во время Второй мировой войны этот фронт простирался уже за тысячи километров от линий боевого соприкосновения и глубоко затрагивал многие стороны государственной жизни.

40-е годы прошлого столетия стали временем демонстрации выдающейся роли криптографии в сфере военного управления. Вскоре последовало и признание её оборонной значимости наравне с ракетно-ядерным оружием.

ВЫРОСЛА ЗНАЧИМОСТЬ ДЕШИФРОВАЛЬНОЙ РАБОТЫ

Поскольку противоборствующие стороны активно внедряли шифрование на своих линиях связи, то возросла и значимость дешифровальной работы. В предшествующий и начальный период Великой Отечественной войны такая работа в СССР велась специально созданными подразделениями НКВД, ГРУ Генштаба РККА и в дешифровально-разведывательной службе ВМФ. По мобилизации в состав Генштаба была зачислена большая группа молодых математиков, физиков, инженеров, лингвистов, немало из которых имели учёные степени кандидатов

наук. В дальнейшем они сыграли существенную роль в развитии криптографии и в подготовке специалистов-криптографов.

Среди этой группы были В.С. Полин, Г.И. Пондопуло, М.И. Соколов и многие другие. Их свежие идеи вскоре пригодились. Так, В.С. Полин (1907–1975) стал конструктором и организатором применения вспомогательного оборудования для дешифрования. Эта техника тогда представляла собой отдельные рележные или многоламповые устройства, облегчавшие трудоёмкие процессы статистического анализа материалов шифрперехвата. В условиях нехватки кадров основной упор в дешифровальной работе по военной линии был сделан на вскрытие шифрпереписки войсковых сетей немецкой армии, органов военной разведки и войск СС, а также переписки немецкой полевой полиции и жандармерии.

В ноябре 1942 года дешифровальная служба военной разведки была передана из Генштаба в НКВД. В декабре 1942 года на базе прежних школ Генштаба и НКВД, готовивших дешифровальщиков, организовали Специальную школу Пятого Управления НКВД в составе двух отделений с 10-месячным сроком обучения и был создан Криптографический совет. Два отделения школы готовили кадры для



Иллюстрация 1.
Владимир Степанович Полин



Иллюстрация 2.
Георгий Иванович Пондопуло



ФОНД
ПРЕЗИДЕНТСКИХ
ГРАНТОВ

Публикация подготовлена при поддержке гранта Президента Российской Федерации на развитие гражданского общества №21-1-009977, предоставленного Фондом президентских грантов

дешифрования военной и дипломатической переписки соответственно. В этой спецшколе в 1943 году был издан первый «Криптографический сборник» под редакцией Б.А. Аронского, С.С. Толстого и А.В. Австриакова. Сборник содержал 13 статей с описанием аналитических методов раскрытия ручных шифров и кодов. Специальная школа и криптографические подразделения, находившиеся в Уфе, подчинялись А.И. Копытцеву, в недавнем прошлом аспиранту мехмата МГУ, уже ставшему одним из руководителей дешифровальной службы НКВД.

КРИПТОГРАФИЧЕСКИЙ ЩИТ ОТЕЧЕСТВА

При всей значимости дешифровальной работы особой государственной заботой являлось обеспечение секретности при передаче важной информации по каналам связи. За годы войны только шифровальная служба Генштаба РККА разослала нижестоящим штабам и войскам порядка 3,2 млн комплектов шифрдокументов.

Криптографы противоборствовавших сторон проделали гигантскую работу по обеспечению безопасности проводной связи и радиосвязи для военных и гражданских нужд в масштабах значительной части земного шара. Ведь шифрование применялось даже в такой неожиданной области, как передача метеосводок. Как и во всех воевавших государствах, в СССР связь по линии Гидрометеослужбы была засекреченной, поскольку эта информация представляла большую ценность. Документ с интернет-сайта «Память народа» на илл. 3

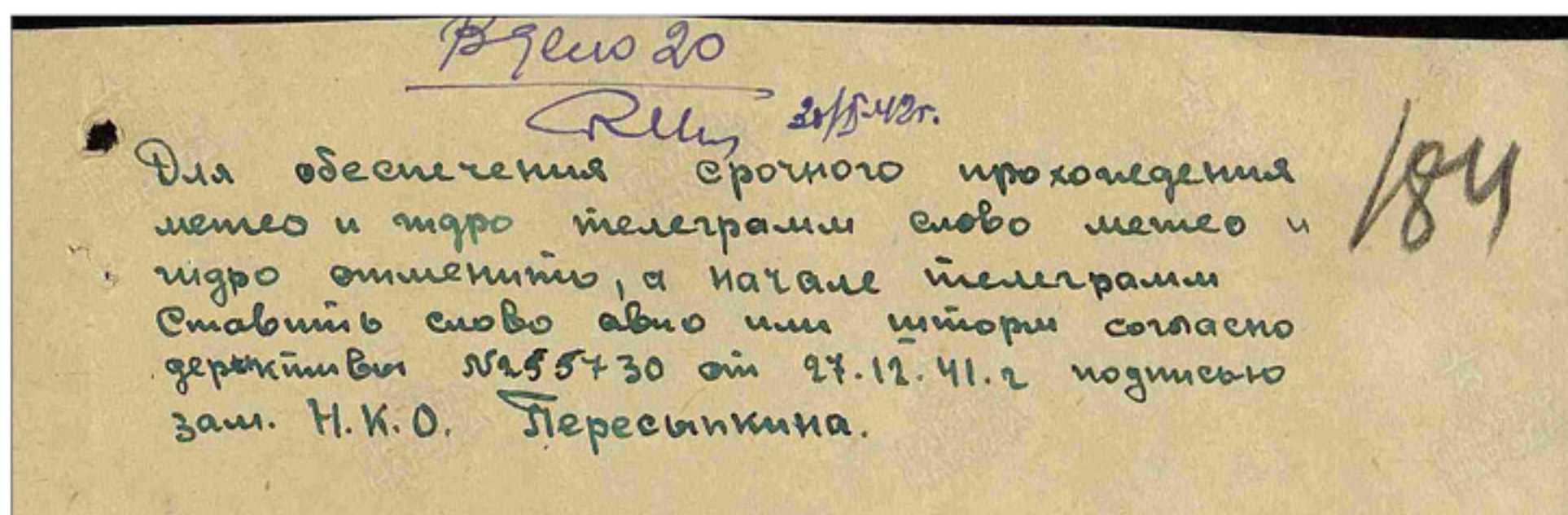


Иллюстрация 3. Директива ГУ Связи Красной Армии. Источник: pamyat-naroda.ru

Иллюстрация 4. Переговорная гидрометеорологическая таблица периода Великой Отечественной войны. Источник: pamyat-naroda.ru

ДОПОЛНЕНИЕ ДЛЯ ТЕХ, КОМУ ИНТЕРЕСНО

Как применять практически такую таблицу, посмотрим на примере. Предположим, что 10 клеток свободного левого столбца (назовём его ключевым столбцом) заполнены сверху (пропуская самую верхнюю клетку) вниз парами чисел **90, 85, 13, 40, 37, 50, 58, 00, 10, 03**, а 10 клеток свободного верхнего ряда (назовём его ключевым рядом) заполнены слева (пропуская самую левую клетку) направо парами чисел **80, 75, 05, 40, 49, 38, 25, 90, 03, 08**, и расшифруем такое начало сообщения:

5008 0338 5049 9080 3749 9049 1049 1038 8540 5849 1038 9080 1380 9090¹...

Каждую четырёхзначную группу чисел мысленно разобьём на две пары. Первую пару ищем в ключевом столбце, а вторую — в ключевом ряду. Первая группа чисел **5008** составлена из пары **50**, стоящей на шестом месте в ключевом столбце, и пары **08**, стоящей на десятой позиции в ключевом ряду. Поэтому расшифровку для **5008** мы должны найти в клетке, расположенной на пересечении шестой строки и десятого столбца таблицы. Там указано «прогноз погоды». Для группы чисел **0338** смотрим пересечение десятой строки и шестого столбца таблицы, там стоит «на». Аналогично расшифруем **5049** как «14», здесь из трёх вариантов мы по умолчанию указаний выбрали первый. Для **9080** имеем значение «буквенная передача». Стало быть, далее будет возможен выбор, и следует выбирать буквенный вариант. Действительно, для **3749** возможны либо число «13», либо буква «о», либо «окопы», выбираем «о». Для **9049** находим «к», для **1049** — «т» и т.д. В результате читаем: «Прогноз погоды на 14 октября...».

¹ Приведённые здесь переговорная таблица и числовые данные использовались организаторами московской интернет-олимпиады «Готов к жизни в умном городе» (май 2020 г.) при составлении видеозаданий для школьников

свидетельствует о приоритетной передаче телеграмм с гидрометеоданными.

Во фронтовых условиях для связи использовали ПГМТ — переговорные гидрометеотаблицы, одна из них представлена на илл. 4.

В свободных клетках таблицы (слева и вверху) записывали двузначные числа — очередной ключ шифра. Таким образом, каждая внутренняя клетка таблицы получала четырёхзначное числовое обозначение, и прогноз погоды можно было передать последовательно четырёхзначных числовых групп.

ОСНОВНАЯ НАГРУЗКА ЛЕГЛА НА МАШИННУЮ ШИФРСВЯЗЬ

Велика, разумеется, была потребность в шифровальных кадрах. За время ВОВ Курсы усовершенствования командного состава, а также учебные команды фронтов и военных округов подготовили и отправили на фронт более 5 тысяч специалистов-шифровальщиков.

Чувствителен был недостаток специалистов высокой квалификации, способных к разработке новой шифртехники и обучению шифровальщиков. В предвоенные годы основы криптографии преподавались в Военно-инженерной академии имени В.В. Куйбышева в Москве и в Военной академии связи в Ленинграде. Их выпускники и пополняли в основном ряды создателей новой шифртехники. А ведь офицеры-конструкторы из ГШ РККА в годы войны занимались не только созданием новых технических образцов, но и внедрением их в войска, обучением работе во фронтовых условиях.

На машинную шифрсвязь в годы войны легла основная нагрузка при передаче секретных телеграмм. Только в ГШ РККА за военный период было обработано свыше 1,6 млн шифртелеграмм и кодограмм. К концу 1944 года в 130 шифрорганах Красной Армии имелись на вооружении шифровальные и кодировочные машины.

Разработкой шифртехники занимались также в НКВД и промышленности. Как известно, в предвоенное время государственные и партийные инстанции стимулировали это направление оборонного строительства притоком выпускников вузов с хорошей математической и физико-технической подготовкой. Такое



Иллюстрация 5. В.А. Котельников

качественное пополнение, усилившееся мобилизацией с первых дней войны, в дальнейшем принесло плоды. Но начало войны многое и осложнило.

В.А. Котельников вспоминал, что при приближении фронта к Москве ЦНИИС Наркомата связи, где он трудился, был распущен, а все сотрудники уволены. Оставили только его лабораторию, поскольку там велись работы по закрытой радиотелефонии, так необходимой для фронта. Им было поручено получить деньги и расплатиться со всеми уволенными сотрудниками института. Затем следовало сжечь всю документацию, кроме самой важной, и подготовить оборудование лаборатории

к эвакуации в Уфу. На новом месте работа осложнилась тем, что была уничтожена значительная часть конструкторской документации. Несмотря на все трудности, уже к осени 1942 года было изготовлено несколько образцов аппаратуры секретной радиотелефонии. Их сразу же направили на Закавказский фронт, с которым временно прервалась проводная связь. Как известно, уже к началу 1943 года было налажено производство новой аппаратуры, а затем и использование её в действующей армии. Тогда не существовало более стойкой аппаратуры закрытой радиотелефонии. Вскоре это достижение было отмечено Сталинской премией 1-й степени.



Иллюстрация 6. Корпус А главного учебного здания МЭИ в 1945 году (pastvu.com)

«ВАМ НЕОБХОДИМО ЗАЩИТИТЬ ДИССЕРТАЦИЮ»

Весной 1943 года лаборатория В. А. Котельникова была разделена, часть её отозвали из Уфы в Москву и перевели в распоряжение НКВД. В этот момент Котельникова разыскала Валерия Алексеевна Голубцова — новый директор (ректор) МЭИ. Война была в разгаре, но страна уже приступала к восстановлению разрушенного народного хозяйства. Начал активно восстанавливаться и МЭИ, в ту пору единственный действующий электротехнический вуз, стране остро требовались специалисты. Рассказав о перспективах развития института, В. А. Голубцова (илл. 7) предложила Котельникову вернуться в МЭИ, и Владимир Александрович с готовностью согласился, поскольку предпочитал заниматься наукой в гражданском учреждении. Надо сказать, что В. А. Голубцова была женой крупного государственного руководителя, члена Политбюро и секретаря ЦК ВКП(б) Г. М. Маленкова. По-видимому,

благодаря этому и удалось Владимиру Александровичу, будучи руководителем разработок с секретной тематикой, перейти из системы НКВД в МЭИ. Правда, Котельников продолжал заниматься вопросами секретной связи в ЦНИИС НКС. В. А. Голубцова (1901–1987) была незаурядным организатором, она оставила яркий след и в творческой биографии В. А. Котельникова.

Приказ о переводе в МЭИ на должность заведующего кафедрой «Основы радиотехники» был подписан 1 ноября 1944 года. Позднее Владимир Александрович был избран ещё и деканом РТФ, объединив коллектив талантливых учёных и инженеров. В 1944–1947 годах они разрабатывали телеметрическую аппаратуру для самолётов. Новая телеметрия получила высокую оценку, а Котельников был удостоен второй Сталинской премии 1-й степени за создание систем специальной связи.

Весной 1946 года В. А. Голубцова вызвала как-то Котельникова и настоятельно рекомендовала: «Владимир



Иллюстрация 7. В. А. Голубцова, ректор МЭИ в 1943–1952 годах

Александрович, Вам необходимо защитить докторскую диссертацию». Котельников вспоминал, что никаких идей насчёт темы диссертации у него тогда не было. Летом, взяв очередной отпуск, он принялся сочинять «Теорию потенциальной помехоустойчивости» — так была озаглавлена диссертация, содержание которой было навеяно его прежними работами в секретной

радиотелефонии и новыми — в радиолокации. Осенью диссертация была готова. Но подыскать оппонентов оказалось непросто, позднее о диссертации отзывались так: «Она появилась для научной общественности буквально на пустом месте».

Действительно, в работе Котельникова впервые были проанализированы основные проблемы связи с теоретико-вероятностных позиций. Близкая по замыслу работа К. Шеннона появилась позже, в 1948 году. Снова выручила Голубцова, оппоненты были найдены, и в январе 1947 года состоялась защита. Ныне признано, что эта диссертация дала мощный импульс для развития статистической теории передачи сообщений, для разработки эффективных способов функционирования приёмных устройств, что было очень актуально. Вскоре началась захватывающая работа в рамках Ракетно-космической программы страны, в которую активно включился и МЭИ.

КОСМИЧЕСКИЕ ПЕРСПЕКТИВЫ

Как известно, 1945–1949 годы стали временем важных государственных решений, связанных с созданием ракетно-ядерного щита СССР. Так, 20 августа 1945 года был образован Спецкомитет, призванный руководить всеми работами по атомной проблематике (Комитет № 1). 19 мая 1946 года Сталин подписал постановление о создании в Советском Союзе ракетной отрасли промышленности, техники и науки (Комитет № 2). Вскоре подошёл черёд радиолокации, систем управления и всего радиоэлектронного вооружения. Соответствующее постановление о Спецкомитете (Комитет № 3) было подписано 10 июля 1946 года. Партийное руководство 2-м и 3-м Комитетами возложили на Г. М. Маленкова. Из воспоминаний участников реализации этих решений известно о гигантских усилиях, предпринятых для создания новых производств, для объединения исследований академической, отраслевой и вузовской науки, а также для подготовки новых кадров.

В частности, был создан головной институт по ракетной технике в

Подлипках, вошедший в историю под именем НИИ-88, ныне это ЦНИИ машиностроения — интеллектуальный центр Госкорпорации «Роскосмос». Б. Е. Черток, бывший заместитель главного инженера НИИ-88 по системам управления, много позже вспоминал, как в начале апреля 1947 года в институт для ознакомления с его работой приехал президент Академии наук СССР Сергей Иванович Вавилов.

«Сергей Иванович приехал не со свитой академических учёных, а с директором МЭИ В. А. Голубцовой. Ознакомившись с проблемами, которые тогда требовали активного участия учёных разных направлений, Вавилов высказал мысль о необходимости создания в системе Академии наук специального Института — будущего Института космических исследований... В. А. Голубцова, в свою очередь, предложила, чтобы я, бывший студент и аспирант МЭИ, приехал в свой родной институт и рассказал учёным института о наших проблемах. Буквально на следующий день я приехал в МЭИ. Там была собрана группа учёных, возможно, Учёный совет, который вела сама Валерия Алексеевна. Я рассказал об основных проблемах, которые стояли перед нами, хотя мы сами мало ещё понимали, в чём эти проблемы, дело было ещё только на стадии становления. На следующий же день Голубцова ещё раз вызвала меня и посадила в компанию, в которой находился в качестве руководителя, как я понял, заведующий кафедрой «Основы радиотехники» В. А. Котельников. И тогда я рассказал, что для нас сегодня самое важное — это иметь возможность с помощью радиотехнических средств непрерывно в реальном времени получать параметры ракеты... Всего через 10 дней после нашей встречи в кабинете Голубцовой, 27 апреля 1947 г., вышло постановление правительства, подписанное Сталиным, о создании в МЭИ совершенно секретного Сектора специальных работ для выполнения НИР в интересах реактивного вооружения. Даже для нас, привыкших к оперативным решениям правительства, столь быстрая и эффективная реакция была впечатляющей.

Руководителем Сектора специальных работ был назначен Владимир



Иллюстрация 8. В. А. Котельников и Б. Е. Черток на конференции «10 лет полёту „Бурана“»

Александрович Котельников... Все первые полёты, вошедшие в историю ракетной космической техники, проходили с непременным использованием радиотехнических устройств, созданных школой Котельникова. Имеется в виду и бортовая, и наземная радиотехническая аппаратура. И что очень важно — телеметрическая аппаратура, которая непрерывно посылает на землю все параметры, интересующие и разработчиков, и тех, кто эксплуатирует космические аппараты».

Предыдущие разработки авиационной телеметрии и засекреченной связи хорошо подготовили В. А. Котельникова к новым решениям, хотя требования к аппаратуре для применения в ракетных полётах заметно выросли. Спецсектор быстро добился независимости от промышленных министерств при изготовлении разрабатываемых систем, создав при МЭИ свои опытные мастерские, а затем и завод с законченным циклом. Перспективы открылись необъятные, космические.

«ПРОДОЛЖАЙТЕ СПОКОЙНО РАБОТАТЬ»

Когда осенью 1947 года Котельникова вызвали к министру государственной безопасности СССР В. С. Абакумову, бывшему начальнику СМЕРШа, Владимир Александрович, вероятно, подозревал, о чём пойдёт речь. Как вспоминал Котельников, разговор проходил в очень вежливом и уважительном тоне. Рассказав о создании Специальной лаборатории в Марфино, Абакумов предложил Владимиру Александровичу возглавить её. Когда тот отказался,



Иллюстрация 9. Здание Специальной лаборатории в Марфино

министр удивился и поинтересовался причиной несогласия. Котельников объяснил, что хочет заниматься наукой в вузе. Абакумов безуспешно попытался его уговорить, пообещав множество привилегий. В конце концов министр заключил: «Ну что ж, а жаль» — и они распрощались. Возвратившись в МЭИ, Котельников сразу пошёл к ректору Голубцовой и рассказал о визите в МГБ. Выслушав, она спросила, чего хочет сам Владимир Александрович. После ответа: «Работать в МЭИ» Валерия Алексеевна сказала: «Тогда продолжайте спокойно работать».

Вскоре В. А. Котельников как главный конструктор Спецсектора вошёл в межведомственный Совет главных конструкторов, который возглавлял С. П. Королёв.

Конечно, Котельников являлся прежде всего выдающимся учёным и инженером XX в., одним из основоположников цифровой техники анализа сигналов, статистической радиофизики и радиотехники, радиолокационной астрономии. Но в широкий круг его интересов входили также и надёжное шифрование многоканальной телеметрии, и секретная телефония. Он не только продолжал консультировать разработчиков новой телефонной засекречивающей аппаратуры, но и принимал участие в работе Государственной комиссии по приёмке опытных образцов. Как известно, криптографически стойкая аппаратура для засекречивания

телефонной информации, использовавшая результаты исследований по дискретизации речевого сигнала и оригинальный вокодер, была создана в 1950-х годах.

ВЫСОКИЙ СТАТУС ПРОБЛЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В конце 1940-х годов руководство СССР вполне осознавало необходимость преобразований в шифровальной деятельности. Стали ясны и крупные масштабы предстоящего развития такого направления. Ведь обеспечение эффективности создаваемого ракетно-ядерного щита требовало гарантированной защиты от попыток противника преодолеть его. Необходимо было исключить любую возможность для несанкционированного доступа к системам управления и бортовой телеметрии, а значит, вся полётная информация нуждалась в надёжном шифровании. А в условиях уже складывавшегося глобального радиоэлектронного контроля следовало предусмотреть возможность гарантированной защиты всей государственно важной информации. Можно представить себе, какие силы и средства были необходимы, чтобы развернуть разработку, производство и широкое внедрение шифровальной техники, развитие научные направления криптографии, наладить подготовку кадров. И, несмотря на тяжёлое экономическое положение, руководители СССР посчитали жизненно важным приоритет задач



Иллюстрация 10. В. А. Котельников

защиты информации наряду с ракетно-ядерной проблематикой.

Вскоре после успешного испытания советской атомной бомбы было создано ГУ Специальной службы (ГУСС) при ЦК ВКП(б). Такое подчинение подчеркнуло особую значимость защиты информации и нового ведомства. Оно возникло на основе 6-го Управления (шифрование-дешифрование) МГБ и дешифровально-разведывательной службы ГШ Вооружённых сил. Как известно, соответствующее постановление Политбюро вышло 19 октября 1949 года. Вскоре было активизировано создание стойкой к дешифрованию секретной телефонии и высокоскоростных шифраторов, а также специализированной вычислительной техники. В криптографию привлекли ведущих специалистов Академии наук и вузов. При механико-математическом факультете МГУ организовали специальное отделение по подготовке математиков-криптографов. Одновременно в структуре ГУСС было создано специальное высшее учебное заведение по подготовке криптографов и специалистов математического, физико-технического и связного профиля. Его преемником является ныне Институт криптографии, связи и информатики. Крупные силы, ресурсы и богатые научные традиции обеспечили постепенный выход советской криптографии на передовые позиции в мире.

**Роман МЕЩЕРЯКОВ**

главный научный сотрудник
Лаборатории №80
киберфизических систем
ИПУ РАН, доктор технических
наук, профессор

**Валерия МЕЩЕРЯКОВА**

выпускница факультета
журналистики МГУ
имени М.В. Ломоносова

ОТ ЧАЙНИКА ДО КИБОРГА

ОТЕЦ И ДОЧЬ ПЬЮТ ЧАЙ НА КУХНЕ И РАЗГОВАРИВАЮТ ПРО ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И БЕЗОПАСНОСТЬ

Не будем скрывать, *BIS Journal* нещадно эксплуатирует родственные связи своих сотрудников. И в первую очередь связи Валерии Мещеряковой — выпускницы факультета журналистики МГУ, заведующей на страницах журнала молодыми безопасниками. Точнее, тем коротким, но страшно ответственным отрезком жизни, на котором многочисленные студенты факультетов ИБ всего мира превращаются в немногочисленных специалистов сферы ИБ. Надеемся, её цикл интервью и репортажей из России и Франции, посвящённых перипетиям юных в поисках работы в ИБ, себя в ИБ и ИБ в себе, привлёк внимание наших читателей. Так вот, периодически редакция даёт своему молодому корреспонденту задание упорядочить и обобщить собственные впечатления в беседе с Романом Мещеряковым — своим папой, а по совместительству главным научным сотрудником Лаборатории 80 киберфизических систем ИПУ РАН, доктором наук, профессором и проч. и проч. В последний раз получилось весьма познавательно¹.

На этот раз дочь расспрашивает отца об искусственном интеллекте.

¹ «В России нет понимания профессии безопасника. Отец и дочь беседуют о проблемах образования в сфере ИБ», *BIS Journal* № 1(32)/2019

— Мы живём в интересное время — иногда кажется, что вещи умнее нас с тобой. Звонишь в банк — отвечает голосовой помощник, который знает наши проблемы лучше нас самих, а умный дом — вообще райское место: интеллект есть даже у стиральной машины, даже у чайника, из которого мы с тобой сейчас пьём...

— Да, желание встроить технологии во всё, что возможно, превышает мыслимые пределы — развитие идёт по областям Industry 4.0, IoT (IoE), BigData и т.п. И да, любые продукты и услуги, использующие вычисления, обработку данных, сегодня пытаются отнести к системам с искусственным интеллектом.

— Но так ли всё радужно, как нам говорят?

— Хорошо, давай обсудим и помечтаем, и прости, если буду использовать специфические термины.

— Итак, что же такое искусственный интеллект?

— Существует огромное количество определений искусственного интеллекта. Из всех этих определений следует, что основные области применения технологий искусственного интеллекта — это системы обработки информации для задач, которые человек решает просто, но они слабо поддаются формализации либо относятся к NP-полным задачам. Тут следует привести английский термин — Artificial intelligence, переводимый на русский язык как искусственный интеллект. Однако его семантическое поле определяется гораздо шире: Intelligence — Artificial intelligence — Intellect. Следовательно, надо воспринимать этот перевод не как один термин, а как некоторое облако понятий и смыслов. Также не будем отвлекаться на понятия слабого (для решения узких задач) и сильного (общего назначения) искусственного интеллекта.

Попытка заменить естественный интеллект искусственным давно занимает человечество. Издревле люди хотели,

чтобы машины мыслили. И тут существуют два подхода. Один — механистический, включающий в себя попытки физического моделирования нервной системы или её элементов, опыты на насекомых, млекопитающих и всяческое биологическое моделирование. Другой — вычислительное моделирование, то есть создание вычислительных структур и процессов, которые информационно моделируют процессы размышления.

Не будем углубляться в детали технологий искусственного интеллекта, но нужно понимать, что сегодня существует огромное множество методов, которые в этом направлении используются, и они не ограничиваются искусственными нейронными сетями, которыми, кстати, много где занимаются, причём с разной степенью успешности и разными объёмами финансирования.

— А как же информационная безопасность?

— Выполнение требований информационной безопасности ориентировано

на обеспечение защиты свойств информации: конфиденциальности, целостности и доступности. Сформулируем попроще: нужно, чтобы информация не выходила за пределы определённого круга лиц и систем, была неизменна и к ней был доступ в течение разумного количества времени. Конечно же, свойств у информации, которой требуется защита, гораздо больше (например, часто важно авторство), но не будем отклоняться от курса.

Первое, что делается для защиты информации в различных системах, — это категоризация информации и проведение аудита. Современные системы и средства защиты активно разрабатываются для противодействия новым видам атак и нарушителей. Вместе с тем системы обработки информации становятся более сложными, а при увеличении сложности возрастает и количество уязвимостей.

— **И какие перспективы у искусственного интеллекта в сфере защиты информации?**

— С одной стороны, технологии искусственного интеллекта можно использовать на стороне атаки, с другой — для защиты информации. Варианты использования технологий искусственного интеллекта для атак опустим как неэтичные, но будем помнить, что враг преследует свои цели и не всегда поступает морально. Примером такого рода атак являются дипфейки, в которых реальное видео и голос заменяются чужими.

Для обеспечения защиты информации распространены технологии искусственного интеллекта, которые проводят анализ данных на предмет выявления вредоносного содержимого (в статике) или проведения несанкционированных действий (в динамике). Для этого как создаются математические модели и алгоритмы, так и разрабатывается специализированное аппаратное обеспечение, ориентированное на использование алгоритмов.

— **А можно ли верить результатам работы систем с искусственным интеллектом?**

— В сферах, где обрабатывается и используется информация, которая незначительно влияет на окружающий мир, требований к правилам

функционирования нет. Однако в финансовых и оборонных системах, в здравоохранении ошибки могут привести к значительным последствиям. Следовательно, надо каким-то образом оценивать их работу и требовать доверия к системе.

В классических подходах, как правило, изначально имеется модель, в которой заложена доказательная составляющая, что формирует так называемую доказуемую стойкость шифра — давай вспомним правило Кирхгофа.

В настоящее время имеются такие основные подходы.

◆ Тест Тьюринга, в котором человек взаимодействует с одним компьютером и одним человеком и на основании ответов на вопросы определяет, с кем он разговаривает. В этом случае тест показывает, насколько компьютер с ИИ может имитировать размышления человека.

◆ Система интерпретации поведения и размышления ИИ. Внешняя (по отношению к системе с искусственным интеллектом) система проводит оценку выполнения «рассуждений» ИИ, и в зависимости от степени интерпретируемости система с ИИ признаётся заслуживающей доверия или нет.

◆ Проверка решений на верифицированных базах данных. Например, можно провести проверку системы оценки степени поражения по медицинским изображениям на верифицированных данных.

Собственно, отсутствие достоверности (гарантий) работы систем с ИИ сильно сдерживает их внедрение в системы безопасности и другие автономные системы.

— **А можно ли как-то воздействовать на системы с искусственным интеллектом?**

— Системы с искусственным интеллектом обладают некоторыми специфическими уязвимостями. Как правило, для систем с ИИ готовится обучающая выборка. Гарантий, что выборка полна и в ней присутствуют все возможные комбинации для классификации событий, вряд ли кто-то даст.

Что может случиться или пойти не так? Большую проблему несёт в себе появление в обучающей выборке специально подготовленных данных с

аномалиями, которые не могут быть распознаны на этапе обучения. С другой стороны, мир меняется, и с течением времени требуется дообучать систему под новые реалии, и система начинает заметно отличаться от своего исходного состояния.

Следующая проблема — это собственно атаки на систему. Один из самых известных примеров атак — это когда на рисунок с купюрой низкого номинала накладывается шум, и она распознаётся как купюра с высоким номиналом (ну, прям как классический пример панды с гиббоном). И примеров таких много.

Сейчас злоумышленнику не нужно подделывать голос — проще сразу атаковать биометрическую систему речеподобным сигналом.

Важно, что в системах с искусственным интеллектом мы получаем системную закладку, и когда она срабатывает, мы не знаем. Получается, что формально вся входная информация проверяется и проходит детекторы, однако при сборке в системе появляется закладка.

— **Значит, слухи о возможностях искусственного интеллекта сильно преувеличены. И всё же, какие у него перспективы?**

— Несмотря на недостатки систем с искусственным интеллектом, технологии развиваются, и их необходимо использовать. А новые вычислительные архитектуры, микропроцессоры, телекоммуникационные каналы связи, источники энергии на новых материалах (включая квантовые и оптические системы) позволят существенно повысить эффективность работы существующих технологий с искусственным интеллектом.

Вместе с тем мы живём, и мир вокруг значительно меняется. Так, всё больший упор делается на инвазивные интерфейсы систем взаимодействия человека с компьютером, и вполне возможно, что человек уже свернул в сторону киборгизации — для расширения своих возможностей и повышения эффективности. В общем, жизнь будет более сложной и менее контролируемой, а работа специалиста по информационной безопасности — более интересной.

УПРАВЛЯТЬ НЕ УМЕЕМ МОНИТОРИТЬ

ЗАМЕТКИ БЕЗОПАСНИКА



**Александр
БОДРИК**
эксперт BIS Journal

Известное «казнить нельзя помиловать» как нельзя лучше применимо к ситуации в службах информационной безопасности. При очередном стимуле извне — регуляторном окрике или приходе новой технологии — службы ИБ начинают метаться, задаваясь вопросом: **управлять или мониторить?**

Вопрос можно назвать вечным. Например, автор сталкивается с его многочисленными реинкарнациями и их

пульсирующими следами ещё с 2003 года и начинает считать его всё более одиозным, то есть не столько вечным или вечно актуальным, сколько опасно навязчивым для нервной системы безопасника.

Итак, **управлять или мониторить?** Для примера возьмём Active Directory, в работе которой иностранный регулятор нашёл недостатки, и служба ИБ иностранной компании раздумывает, не взять ли её под управление.

ЗА

УПРАВЛЯТЬ НЕ УМЕЕМ, МОНИТОРИТЬ

- ♦ службы ИБ обычно не имеют достаточного масштаба (сил и средств) для поддержки 24×7 ключевых ИТ-сервисов;
- ♦ по этой же причине у служб ИБ, как правило, не развиты эксплуатационные процессы, нет круглосуточной поддержки и практически отсутствует культура uptime-fist;
- ♦ управление ИТ-сервисами размывает фокус информационной безопасности и перегружает и так перегруженного CISO.

- ♦ уровень формализации процессов поддержки силами ИТ не всегда позволяет доказать регуляторам, что управление ключевыми сервисами авторизации и аутентификации происходит профессионально;
- ♦ замедление времени реагирования на инциденты.

ПРОТИВ

ЗА

УПРАВЛЯТЬ, НЕ УМЕЕМ МОНИТОРИТЬ

- ♦ найти инженеров по управлению Active Directory гораздо проще, чем SOC-аналитиков;
- ♦ SOC может иметь очередь use cases на годы вперёд и без детальной проработки Active Directory (как цинично для многих технических экспертов это ни звучит);
- ♦ лучший контроль за загрузкой инженеров Active Directory повысит вероятность наличия у них времени на тщательное ухаживание за своим AD-огородом.

- ♦ мониторить всё равно надо учиться, и делать это быстро — систем всё больше, и все на управление не возьмёшь;
- ♦ инфраструктурная точка отказа в управлении — это неблагодарная работа и бессонные ночи, когда отказ всё же случается.

ПРОТИВ

В целом можно и **управлять**, и **мониторить**, важно помнить два момента. Первый — решение это нужно принять с коллегами, которые, если что, подставят плечо или будут решать ситуацию, если наша

служба ИБ её не потянет. И второй — CISO должно быть комфортно жить с этим решением, поэтому лично я по умолчанию выбрал бы «**управлять не умеем, мониторить**».

XI симпозиум

«Современные тенденции в криптографии»

Тематика симпозиума включает следующие вопросы (но не ограничивается ими):

- исследование криптографических алгоритмов и протоколов, в том числе являющихся международными стандартами;
- эффективная реализация методов анализа криптографических алгоритмов и протоколов;
- оценка криптографической стойкости российских криптографических алгоритмов и протоколов;
- эффективная реализация российских криптографических алгоритмов и протоколов;
- математические аспекты криптографии;
- криптография в «Интернете вещей»;
- квантовая криптография и квантовые вычисления;
- постквантовая криптография;
- криптография и технология блокчейн;
- криптографическая защита биометрических данных;
- другие актуальные и перспективные направления криптографии



ОРГАНИЗАТОРЫ



МИАН

ПРИ ПОДДЕРЖКЕ



ФСРБИТ

ОРГПОДДЕРЖКА



Проекты Медиа Группы «Авангард»

Онлайн и офлайн-мероприятия

Отраслевой журнал BIS Journal

Интернет-телекомпания BIS TV

Энциклопедия безопасника

ib-bank.ru



**Окупись в мир
информационной
безопасности!**



АВАНГАРД